

**GUVERNUL  
REPUBLICII MOLDOVA**

**PROGRAMUL NAȚIUNILOR  
UNITE PENTRU DEZVOLTARE**

**PROIECTUL**  
**IMPLEMENTAREA COMPONENTEI E-GUVERNARE A STRATEGIEI NAȚIONALE**  
**E-MOLDOVA**

**SISTEMUL INFORMATIC CU PORTAL**  
**„e-Declarații”**

**Chișinău 2006**

# Cuprins

## Introducere

Obiectivele documentului

### 1. Analiza problemei

- 1.1 Definiția Sistemului
- 1.2 Scopul și obiectivele Sistemului
- 1.3 Domeniul de aplicare

### 2. Oportunitatea și premisele elaborării sistemului

- 2.1 Structura organizațională a IFpS.
- 2.2 Descrierea și evaluare a sistemului informatic existent
  - 2.2.1 Nivelul de dotare tehnică
  - 2.2.2 Nivelul de informatizare, aria de funcționare a sistemelor existente
  - 2.2.3 Funcții actualmente neîncadrate în sistemul existent
  - 2.2.4 Evaluări referitoare la Sistemul informatic existent, concluzii

### 3 Cerințe față de Sistem

- 3.1 Cerințe generale
- 3.2 Structura organizațională a Sistemului
- 3.3 Structura funcțională a Sistemului
- 3.4 Bazele de Date
- 3.5 Sistemele de programare a aplicațiilor
- 3.6 Sistemul tehnic de prelucrare și transportare a datelor
  - 3.6.1 Sisteme de interconectare Internet / Intranet
  - 3.6.2 Sisteme de transport date adiționale.
  - 3.6.3 Securitatea datelor
- 3.7 Statistica funcționării Sistemului
- 3.8 Interoperabilitatea Sistemului cu alte sisteme informatice (Baze de Date), inclusiv Registrele de Stat  
Cerințe speciale referitor la „comportamentul” Sistemului cu contribuabilii și serviciile prestate acestora
- 3.9 Cerințe speciale referitor la gradul de „deschidere” a Sistemului către portalul central e-Guvernare și Gateway Guvernului
- 3.10 Cadrul normativ-juridic
- 3.11 Parametrii de exploatare ulterioară a Sistemului
- 3.12 Cerințe suplimentare

### 4 Ofertă

- 4.1 Introducere
- 4.2 Motivații pentru elaborare
- 4.3 Obiective
- 4.4 Cerințe față de Sistem
  - 4.1.1 Caracteristicile funcționale
  - 4.1.2 Cerințe de fiabilitate
  - 4.1.3 Condiții de exploatare
  - 4.1.4 Componenta și parametrii resurselor tehnice
  - 4.1.5 Compatibilitate informațională și de sistem
  - 4.1.6 Marcare și ambalaj;
  - 4.1.7 Transportare și păstrare;
  - 4.1.8 Cerințe speciale.
  - 4.1.9 Documente de însoțire
  - 4.1.10 Stadii de elaborare
  - 4.1.11 Ordinea de predare-primire

## **Introducere**

### **Obiectivele documentului “Caiet de sarcini”**

Caietul de sarcini a fost elaborat în cadrul proiectului „Asistența de implementare a componentei e-Guvernare din Strategia Națională de edificare a Societății Informaționale din Republica Moldova”. Conținutul documentului are drept suport studiul de oportunități pentru stabilirea Planului de Acțiuni în crearea și implementarea unui Sistem Informatic în cadrul Inspectoratului Fiscal principal de Stat . Caietul de sarcini a fost discutat și aprobat de Comisia de consultanță a proiectului desfășurat de „Programul Națiunilor Unite pentru Dezvoltare în Moldova”.

Obiectivele prezentului document sunt:

- stabilirea cerințelor față de Sistemului Informatic cu Portal „e-Declarații” al Inspectoratului Fiscal principal de Stat (S. I. „e - Declarații”) referitor la structurile organizațională și funcțională, Bazele de Date (BD) și aplicațiile informatice;
- identificarea surselor de informații pentru completarea și actualizarea BD centralizate;
- determinarea structurii, principiilor de distribuire și volumului fluxurilor informaționale;
- determinarea principiilor de realizare a relațiilor dintre beneficiarii Sistemului și administratorii acestuia;
- determinarea principiilor de colectare, introducere în Baza de Date (BD) a datelor și distribuirea sarcinilor de prelucrare;
- determinarea domeniului (arealului) de funcționare și aplicare a Sistemului.

## **1. Analiza problemei**

### **1.1 Definiția Sistemului**

Sistemul informatic cu portal al Inspectoratului Fiscal principal de Stat „e-Declarații” este preconizat pentru colectarea, depozitarea și prelucrarea dărilor de seamă fiscale ale contribuabililor (persoane juridice și fizice) . Sistemul informatic în varianta propusa va respect principiile de baza și va include în sine componentele prevăzute în concepția de implementare e-Guvernare.

Sistemul Informatic “e-Declarații” constituie mulțimea mijloacelor metodologice și informatice de realizare a funcțiilor ce țin de crearea, administrarea și consultarea Bazei de Date referitoare la relațiile Inspectoratului Fiscal principal de Stat cu subiecții „din afară”: contribuabilii, instituțiile superioare de stat, alte instituții, inclusiv de realizare a funcțiilor:

- completarea și administrarea la Inspectoratul Fiscal Principal de Stat (IFpS) a Bazei de date centralizate;
- recepționarea de la subiecții Sistemului, din cadrul Inspectoratului și „din afară”, prin intermediul rețelelor WAN, a datelor referitoare la activitățile și achitățile (contribuțiile) efectuate;
- consultarea de către subiecții „din afară” a BD centralizată a IFpS;
- asistența informațională continuă a conducerii și specialiștilor IFpS în procesul desfășurării activităților lor;
- realizarea interfețelor Sistemului informatic „e - Declarații” și alte sisteme informatice existente, necesare IFpS în exercitarea funcțiilor sale;
- crearea și administrarea arhivei;
- crearea și administrarea arhivei interne ce ține de funcționalitatea Sistemului.

## 1.2 Scopul și obiectivele Sistemului

Sistemul Informatic “e-Declarații” este destinat :

- creării spațiului informațional unic adecvat scopurilor propuse în activitatea IFpS, inclusiv în realizarea relațiilor sale cu contribuabilii;
- elaborării resurselor informaționale noi, motivate de strategia de dezvoltare a IFpS;
- implementării componentelor Concepției e-Guvernare .

Obiectivele directe ale sistemului preconizat pentru elaborare sunt:

- dezvoltarea principiilor democratice în activitatea fiscală;
- implicarea cetățenilor în limita prevăzută de lege, în activitatea autorităților fiscale;
- accesul la informația publică fiscală;
- sporirea eficacității serviciilor publice fiscale;
- crearea condițiilor pentru antrenarea persoanelor (contribuabililor) în realizarea relațiilor lor cu organele fiscale prin intermediul mijloacelor informatice ale Sistemului;
- realizarea structurii optimale a Bazei de Date (BD) referitoare la activitatea organelor fiscale și „comportamentul” contribuabililor în raport cu organele fiscale;
- reducerea timpului de prezentare a datelor și crearea unui confort pentru contribuabili în realizarea relațiilor lor cu organele fiscale;
- reducerea componentelor birocratice în relațiile „contribuabil-fisc”;
- reducerea timpului de efectuare a procedurilor de acumulare, prelucrare și difuzare a datelor referitoare la activitatea subdiviziunilor IFpS, inclusiv de:
  - de recepționare de la subdiviziunile teritoriale a datelor;
  - de selectare și autentificare a datelor;
  - de generare (opțională, conform indiciilor stabilite) și perfectare a documentelor statistice și analitice;
  - de informare (opțională) a specialiștilor IFpS referitor la activitățile fiscale;
- asigurarea completitudinii, autenticității și veracității datelor;
- asigurarea posibilităților de realizare a interfețelor Sistemului cu alte sisteme informatice, de care beneficiază sau se preconizează pentru elaborare și implementare pentru organele fiscale și cu sisteme informatice „din afara” structurii fiscale.

## 1.3 Domeniul de aplicare

Sistemul informatic “e-Declarații”:

- va fi elaborat și implementat pentru a fi exploatat de către Inspectoratul Fiscal principal de Stat, inclusiv de subdiviziunile sale teritoriale și se adresează conducătorilor și specialiștilor acestora. Sistemul presupune asistența informațională a specialiștilor;
- va servi drept mijloc de realizare a relațiilor „contribuabil – fisc”;
- va servi drept sursă în asistența informațională a instituțiilor superioare de stat;
- va realiza interfețe cu alte sisteme informatice proprii IFpS și altor instituții „din afară”.

Sistemul presupune spațiul informațional „**contribuabili**  $\longleftrightarrow$  **fisc**  $\rightleftarrows$  **alte instituții**”.

Sistemul se definește:

- închis – în raport cu realizarea funcțiilor strict interne ale Inspectoratului Fiscal principal de Stat și subdiviziunilor subordonate;
- deschis – în raport cu prestarea de servicii contribuabililor și difuzarea, prin intermediul rețelelor Internet, a informațiilor publice referitor la activitatea organelor fiscale.

Accesul personalului Inspectoratului Fiscal principal de Stat și subdiviziunilor subordonate la bazele de date administrate de Sistem urmează a fi diversificat conform funcțiilor atribuite.

Accesul altor beneficiari la BD a Sistemului urmează a fi diversificat în funcție de angajamentele organelor fiscale de a asigura complexitatea serviciilor prestate acestor beneficiari.

## 2. Oportunitatea și premisele elaborării Sistemului

### 2.1 Structura organizațională a IFpS

Inspectoratul Fiscal Principal de Stat (IFpS) este organul responsabil de activitatea Sistemului Fiscal în Republica Moldova, subordonat Ministerului de Finanțe.

Structura organizațională a IFpS include următoarele nivele:

- central (IFpS - mun. Chișinău);
- municipiul Chișinău - 6 un. (municipal Chișinău, sec. Botanica, sec. Buiucani, sec. Centru, sec. Ciocana, sec. Rîșcani);
- municipiul Bălți;
- raionale - 32 un. (Basarabeasca, Dubăsari, Anenii Noi, Briceni, Cahul, Cantemir, Călărași, Căușeni, Cimișlia, Criuleni, Dondușeni, Drochia, Edineț, Fălești, Florești, Glodeni, Hîncești, Ialoveni, Leova, Nisporeni, Ocnița, Orhei, Rezina, Rîșcani, Sîngerei, Soroca, Strășeni, Șoldănești, Ștefan Vodă, Taraclia, Telenești, Ungheni);
- Unitatea Teritorială Autonomă Găgăuză - 3 un. (Comrat, Ciadir-Lunga, Vulcanești);
- posturi comune de control - 7 un. ( Anenii Noi, Căușeni, Criuleni, Dubăsari, Florești, Rezina, Ștefan Vodă );

Funcțional aceste subdiviziuni se împart în:

- administrativ-economică (anexa 4);
- control;
- impozitare și urmărire a plăților;
- prelucrare a informației;
- tehnologii informaționale;

Sistemul informatic al Inspectoratului Fiscal principal de Stat funcționează în Direcția tehnologiilor informaționale - 20 pers., care asigura serviciile de proiectare, elaborare, implementare, suport WEB și asistență tehnică.

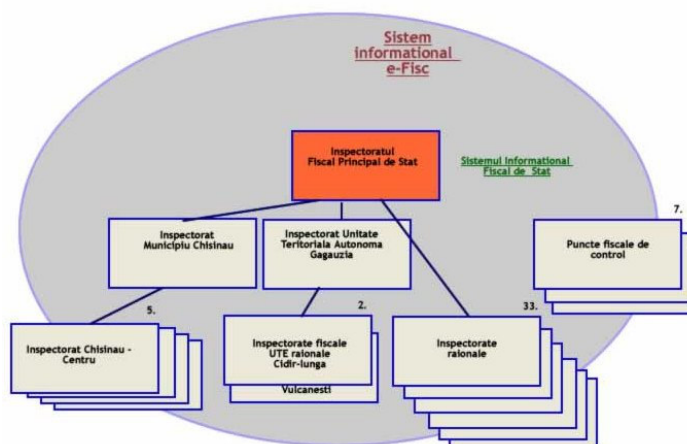


Fig.1 Structura organizațională a Inspectoratului Fiscal principal de Stat.

În Inspectoratul Fiscal Principal de Stat își desfășoară activitatea circa 2285 angajați, 365 din ei sunt angajați ai IFpS.

## **2.2 Descrierea și evaluare a sistemului informatic existent**

### **2.1.1. Nivelul de dotare tehnică**

Infrastructura tehnică a IFpS, modificată în anul 2005-2006, include următoarele:

- PC –uri, rețele LAN, servere și imprimante de utilizare în comun;
- servere cu Risc-procesoare la nivel superior;
- sisteme de depozitare a datelor cu acces multiplu (fiabilitate dublata);
- echipament de rețele pentru linii de comunicație dedicate (CTS);
- sistemul de gestionare a Bazelor de Date (Informix).

Cantitativ, această infrastructură constă din :

- stații de lucru - peste 1000 buc;
- servere cu capacități extinse – peste 40 buc;
- imprimante – peste 670 buc.

Asigurarea locurilor computerizate de muncă în Inspectoratul Fiscal principal de Stat (IFpS) este de 51.6%:

- în IF principal de Stat - 69.7%;
- în IF mun. Chișinău - 54.2%;
- în IF mun. Bălți - 45.4%;
- în IF UTA Găgăuzia - 49,1%.

Sistemul de operare a PC –urilor este Windows 2000 WS sau Windows XP. Toate PC-urile sunt încadrate în rețele locale (LAN ) cu /sau fără conectare la Internet, cu conexiuni la poșta electronică. Serviciu de informare operativă WEB a IFpS este: [www.fisc.md](http://www.fisc.md).

### **2.1.2. Nivelul de informatizare, aria de funcționare a sistemelor existente**

Sistemul informatic existent al Inspectoratului Fiscal principal de Stat este centralizat și prevede colectarea și prelucrarea tuturor dărilor de seamă fiscale. Modalitățile de organizare și modul de prelucrare a documentelor fiscale sunt expuse în documentul de uz intern „Regulament cu privire la modul de organizare și prelucrare centralizată a documentelor în pachete” (martie, 2004).

Ca unitate de informație se utilizează noțiunea de document primar, care include lista documentelor prezentate de Inspectoratele Fiscale pe hîrtie. Documentele în forma de pachete sunt transmise prin poșta oficială la Inspectoratul Fiscal principal de Stat. Procedurile de transmitere, de recepție și de transfer a conținutului documentelor în Baza de Date sunt descrise în regulamentul. Sunt stabilite proceduri de verificare a calității, așa cum ar fi prezența codului fiscal din documente după conținut și forma cu datele din Registrul Fiscal de Stat.

Sistemul informatic existent este funcțional și se utilizează în toate subdiviziunile Inspectoratului Fiscal principal de Stat. Însă, luînd în considerație cerințele actuale pentru un sistem informatic, se face evidentă neadmiterea de către sistemul existent a managementului documentelor electronice, inclusiv a transportării acestora prin intermediul rețelelor WAN.

Documentele în format electronic sunt admise în Inspectoratul Fiscal principal de Stat doar din Trezoreria de Stat, din Trezoreriile teritoriale și de la Casa Națională de Asigurări Sociale. După prelucrare toate tipurile de documente recepționate sunt transmise în Arhiva Fiscală. Numărul documentelor fiscale prevăzute de legislația în vigoare include 166 dări de seamă fiscale. Lista tipurilor de documente primare este expusă în anexa 3.

Reieșind din necesitatea realizării următoarelor obiective puse de Inspectoratul Fiscal principal de Stat în anul 2002:

- securitatea în evidența documentelor;
- utilizarea utilajului și tehnologiilor avansate;
- selectarea specialiștilor bine pregătiți;
- formarea arhivei fiscale republicane;
- sporirea productivității individuale la prelucrarea informației.

a fost implementat sistemul de prelucrare centralizată a datelor.

În baza informațiilor din Bazele de Date Centralizate se creează setul de Rapoarte corespunzător formelor stabilite. Unele informații cu conținut discret se transferă la Inspectoratele fiscale teritoriale pentru activitate administrativă fiscală. Ca instrumente în gestionarea Bazelor de Date Centralizate sunt utilizate:

- sistemul de creare a Bazelor de Date - Informix (ver.10) licențiat pe procesoare;
- sistemul de generare a descrierilor BD - ERWin (ver.1.2);
- sistemul de gestiune a Bazelor de Date - FoxPro;
- sistemul de perfectare a rapoartelor - Crystal Reports.

Prin intermediul sistemului existent au fost prelucrate pînă în prezent estimativ următorul număr de documente:

- 3.9 mln doc. (anul 2003);
- 5.0 mln doc (anul 2004);
- 5.7 mln doc (anul 2005).

Actualmente, din multitudinea funcțiilor, care se încadrează în definițiile enunțate în p. 2 al prezentului Caiet de sarcini, o bună parte au suport informatic în realizare, și anume funcțiile de asistență informațională normativ-juridică a activității tuturor subdiviziunilor și funcțiile ce țin de acumulare în BD a datelor documentelor prezentate de către contribuabili, administrarea BD, generarea de documente rezultative. Astfel, la data demarării lucrărilor de elaborare a Caietului de sarcini, în organele fiscale funcționează, în regim autonom în cadrul rețelelor locale, sistemele informatice .

Fiecare subdiviziune a IFpS, ca și fiecare subdiviziune teritorială, este înzestrată cu tehnică de calcul încadrată în rețele electronice (LAN și WAN), dar utilizarea acestor mijloace nu presupune și realizarea funcțiilor ce țin de prestarea serviciilor contribuabililor cu recurgere la portalul „e Contribuabil”.

### **2.1.3. Funcții actualmente neîncadrate în sistemul existent**

În cadrul Sistemului informatic existent unele funcții și servicii regulamentare prevăzute în concepția de e-Guvernare lipsesc. Acestea sunt:

- funcții de Portal pentru relații publice cu Inspectoratul Fiscal principal de Stat;
- funcții de integrare cu Portalul Central de e-Guvernare;
- servicii de interconexiune la sisteme informatice externe (Registre de Stat, Baze de Date, Sisteme informatice);
- sisteme de utilizare regulamentară a serviciilor Internet;
- sisteme de securizare a comunicațiilor Internet Guvernamental;
- servicii de protejare a comunicațiilor anti-spy și anti-spam;
- servicii de semnătură digitală pentru protejarea și autorizarea circulației datelor;
- servicii publice de Internet pentru comunicații publice.

În afara cadrului sistemului existent actualmente se află realizarea sistematică (continuă) și opțională a funcțiilor:

- administrarea unei BD centralizate (în aparatul IFpS) care ar presupune acumularea directă de la contribuabili a documentelor electronice;
- consultarea, prin intermediul rețelei locale, de către conducătorii și specialiștii aparatului IFpS a BD centralizate constituită din date generalizate (referitor la activitatea sistemului fiscal în ansamblu) și date inițiale (referitor la activitatea subdiviziunii concrete);

- evidență, control și analiză a datelor referitor la „comportamentul” contribuabililor în relațiile lor cu organele fiscale;
- evidența, analiza cantitativă și calitativă a schemelor de personal ale subdiviziunilor teritoriale și aparatul IFpS;
- integrarea serviciilor Web;
- integrarea blog-urilor;
- integrarea unui forum de consultanță pentru persoanele din afara IFpS;
- utilizarea poștei electronice securizate;
- integrarea unui serviciu anti-spam.

#### 2.1.4. Evaluări referitoare la sistemul informatic existent, concluzii

Sistemul informatic existent în Inspectoratul Fiscal principal de Stat poate fi caracterizat ca unul *definit* și *stabil*, cu potențial și posibilități de extindere spre o *integrare deplină*. Concepția de e-Governare ar contribui la crearea unui sistem efektiv și integru interoperabil cu alte sisteme înscrise în această concepție.

Cu toate acestea, reieșind din obiectivele propuse ale Sistemului Informatic „e-Declarații”, funcțiile parțial realizate și cele neîncadrate actualmente pentru realizare, se poate constata că sistemul existent:

- are un suport metodologic și operațional insuficient pentru realizarea relațiilor directe „contribuabil  $\longleftrightarrow$  IFpS” cu recurgere la mijloace informatice;
- poartă un caracter static (indirect) în ceea ce privește realizarea relațiilor directe „contribuabil  $\longleftrightarrow$  IFpS”;
- este inadecvat tendințelor de sporire a fluxurilor de documente transmise/recepționate prin intermediul rețelelor electronice.

Reieșind din analiza succintă a situației existente și concluziile aferente acestei analize se impun următoarele:

- crearea unui Sistem informatic integrat (S.I. „e-Declarații”) cu o structură funcțională completă, având ca suport mijloace informatice de performanță, și care ar funcționa în cadrul rețelelor locale și rețelelor WAN;
- crearea și administrarea în cadrul Sistemului preconizat a bazelor de date alimentate din toate sursele necesare de informații cu tendințe pronunțate către documentele electronice;
- asigurarea accesului reglementat al utilizatorilor la bazele de date ale Sistemului în funcție de strictul necesar pentru exercitarea funcțiilor atribuite;
- asigurarea accesului contribuabilului la bazele de date ale Sistemului în funcție de obligațiunile acestora și interesul organelor fiscale de a stimula onorarea acestor obligațiuni;
- asistența informațională a organelor superioare de stat în funcție de relațiile normativ-juridice ale acestora cu organele fiscale;
- realizarea interfețelor Sistemului informatic integrat „e-Declarații” și alte sisteme informatice necesare IFpS în exercitarea funcțiilor sale.

Premise suplimentare pentru elaborarea și implementarea Sistemului Informatic Integrat „e-Declarații” cu Portal sunt:

- existența unui suport tehnico-operațional (calculatoare, rețele electronice locale, sisteme operaționale și de gestiune a Bazelor de Date, etc.), care datorează unor investiții financiare serioase;
- disponibilitatea IFpS și a subdiviziunilor teritoriale ale lui de un minim suficient de specialiști-utilizatori ai mijloacelor informatice, cunoștințele cărora sunt “congelate” în efectuarea procedurilor de rutină;

### 3. Cerințe față de Sistem

#### 3.1 Cerințe generale

Scopul și obiectivele impuse de Concepția e-Guvernare determină ca Sistemul informatic „e-Declarații” să fie:

- adecvat soluțiilor și cerințelor Concepției de e-Guvernare;
- creat cu orientare proprie critică spre utilizator și serviciile publice prestate;
- scalabil - să asigure capacități de extindere în dependență de cerințe concrete (numărul de tranzacții, volumul de date, numărul de utilizatori);
- interoperabil - să asigure interconexiune, integrare de date, servicii Internet, gestiune a conținutului de metadate cu sistemele colaterale;
- standardizat - în baza standardelor respective ale Uniunii Europene și ale Republicii Moldova;
- asigurat informațional de piața de desfacere a tehnologiilor noi informaționale.

Pentru atingerea scopului și obiectivelor propuse Sistemul Informatic „e-Declarații” trebuie:

- să realizeze integral structura funcțională conform soluțiilor de proiect;
- să asigure continuitatea sistemului informatic existent la data implementării lui (S.I. „e-Declarații”) în vederea acceptării structurii organizatorice a IFpS și subdiviziunilor sale teritoriale;
- să beneficieze de independență structurală și funcțională, având ca surse informaționale:
  - documentele interne (proprii), inclusiv normativ – juridice;
  - documentele, electronice sau pe oricare alt suport parvenite de la alte instituții sau contribuabili.
- să beneficieze de independența structurală, care este exprimată prin posibilitatea modificării (dezvoltării) unui modul fără afectarea altora;
- să respecte standardele tehnologiilor informaționale;
- să asigure utilizarea sistemelor software licențiate, pentru a respecta drepturile la proprietatea intelectuală;
- să permită - prevadă implementarea sistemelor software deschise cu dreptul de a certifica utilizarea lor în sistem;
- să asigure protejarea dreptului de autor pentru componentele noi elaborate în sistem;
- să beneficieze de dreptul de implementare a semnăturii digitale pentru protejarea și autorizarea circulației datelor;
- să asigure flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării după implementare;
- să asigure circulația datelor prin intermediul rețelelor locale și de aplicație largă în funcție de regulamentul stabilit;
- să dispună de o interfață inteligentă și prietenoasă utilizatorului;
- să fie orientat la deservirea unui număr sporit de consultări din partea utilizatorilor, inclusiv în intervale reduse de timp și simultan;
- să recunoască sursele informaționale stabilite, care îl „alimentează”;
- să asigure o fiabilitate înaltă în exploatare;
- să corespundă cerințelor față de securitatea informației;
- să suporte interfețele „utilizator”, „beneficiar” și „alte sisteme” în limba română cu utilizarea caracterelor ANSI-latina 1.

#### 3.2 Structura organizațională a Sistemului

Sistemul informatic cu Portal „e-Declarații” trebuie:

- să dispună de un Portal, pentru a oferi servicii publice de acces contribuabililor;



Portalul „e-Declarații” este parte componentă a sistemului și, prin intermediul mijloacelor software Web Browser, asigură gestiunea proceselor de acces direct (on-line) a utilizatorilor Internet/Intranet.

Portalului „e-Declarații” include în sine un set de aplicații cu destinația - să ofere utilizatorului:

- asigurare informativă - ajutor, școlarizare, informare ;
  - liste de prezență - contacte, adrese de referință;
  - opțiuni de interacțiune cu sistemul;
  - funcțional să asigure;
  - evidență și adaptare a utilizatorilor și a profilurilor;
  - securitate și autentificare de acces;
  - management de conținut;
  - instrumente de creare a formelor pentru prezentarea documentelor;
  - mecanisme de mesaje, care rutează documentele spre destinatar, convertindu-le în formatul sistemelor de destinație;
  - mecanism unitar de reglare, care stabilește regulile de procesare a documentelor;
  - interfață de lucru;
  - aplicație de management a conținutului;
  - structură unitară pentru dezvoltarea, administrarea și mentenanța serviciilor;
- precum și să:
- promoveze o comunicare dinamică și eficientă ;
  - includă instrumente de cooperare în timp real;
  - permită accesul la sisteme de afaceri;
  - gestioneze informații nestructurate;
  - permită să analizeze și să distribuie informații critice pentru afaceri;
  - oferă servicii pentru și gestionarea datelor.

Gateway este parte componentă a sistemului destinată să asigure accesul fiabil și securizat al datelor(informației), prelucrarea datelor(informației) atât prin intermediul aplicațiilor Sistemului „e-Declarații”, cât și prin intermediul aplicațiilor sistemelor informatice colaterale ale sistemului integrat e-Guvernare. Poarta reprezintă resursele tehnice și produsele program, care permit interconectarea sistemelor informaționale existente și asigură accesul la acestea prin Internet.

Arhitectura sistemului de Gateway trebuie să conțină următoarele componente de bază:

- site-urile Web și portalurile departamentelor;
- autentificarea și înregistrarea utilizatorilor (Registration & Enrolment – R&E);
- administrarea tranzacțiilor (Transaction Engine – TxE) și rutarea documentelor;
- integrarea și mecanismul de reglare în baza SOAP și UDDI;
- serverele de interfațare ale departamentelor (Departmental Interface Server – DIS);
- sistem de rutare a mesajelor securizate ( documente XML ).

Prin intermediul de Poarta se asigură următoarele beneficii:

- interacțiunea serviciilor publice;
- securitatea și protejarea accesului la date;
- modul generalizat de prezentare a datelor XML;
- descrierea modului de transformare a datelor din BD;
- asigurarea ajutorului, școlarizării, informării;
- oferirea opțiunilor de personalizare pentru interacțiune;
- servicii de management al rolurilor și profilurilor;
- securitate și protecție împotriva amenințărilor Internetului;

În procesul de elaborare a Planului de Acțiuni urmează să se aprobe o varianta preferabilă, reieșind din prioritățile, avantajele și riscurile de funcționare a sistemului.



Fig. 3. Prezentarea grafică a Sistemului informatic „e-Declarații” cu Portal și Poartă.

### 3.3 Structura funcțională a Sistemului

Reieșind din faptul că Sistemul „e-Declarații” automatizează procedurile ce țin de relațiile „fisc – contribuabil” structura sa funcțională trebuie să fie de tipul „Client ↔ Server ↔ Client”.

Acest tip de structură funcțională presupune centralizarea funcțiilor de administrare fiscală, ceea ce înseamnă crearea la sediul central al IFpS a unei BD centralizate Aceasta înseamnă că activitățile subdiviziunilor de realizare a relațiilor „server ↔ contribuabil” sunt reduse pe seama centralizării acestora de către aparatul IFpS. Structura funcțională trebuie să fie următoarea:

Nr. crt.	Compartiment S.I. „e - Declarații”	Nivel de realizare	Funcție a compartimentului
1	2	3	4
I	Prestare servicii persoanelor fizice și juridice („Contribuabil”)	Server, Baza de Date centrală	Recepționarea și totalizarea dărilor de seamă (rapoartelor statistice)
			Evidența și analiza „comportamentului” contribuabililor la compartimentul „dări de seamă”
			Perfectarea și eliberarea, la cererea contribuabililor, a datelor privind existența/lipsa restanțe
			Crearea și administrarea bibliotecii „Formulare” a dărilor de seamă

			Afișarea la portal a avertizărilor (atenționărilor) către contribuabil referitor la „comportamentul” inadecvat: dări de seamă, achitări ( în cazul accesării portalului de către contribuabil)
			Verificarea veridicității datelor dărilor de seamă prezentate de către contribuabili, și informarea respectivă a acestora
		<b>Portal (Contribuabil)</b>	Identificare contribuabil (cu apel la Registrele de Stat)
			Statistică accesări: (ne)sanționate – compartimente ale BD
			Selectare blocuri meniu
			Selectare proceduri bloc meniu
			Selectare formulare, consultare instrucțiuni respective
			Completare documente
			Lansare documente, confirmare primire de către IFpS și includere în BD
			Extragere din BD a documentelor anterior depuse(prezentate) și consultarea lor cu mențiunile respective. Confirmarea efectuării acestor proceduri
			Extragere din BD a datelor referitor la propriul „comportament” la compartimentul „dări de seamă” pentru perioade opționale
			Afișarea la portal a avertizărilor(atenționărilor) către contribuabil „comportamentului” inadecvat: dări de seamă, achitări ( în cazul accesării portalului de către contribuabil)
<b>II.</b>	<b>Administrarea fiscală</b>	<b>Posturi de muncă instalate în subdiviziunile teritoriale care conlucrează prin intermediul rețelei WAN cu serverul central al IFpS</b>	Mulțimea funcțiilor atribuite subdiviziunilor teritoriale și specialiștilor concreți ai acestora
<b>III</b>	<b>Managementul elementelor de structură organizatorică a IFpS (aparatură IFpS,</b>		Sisteme informatice de management a instituției (de exemplu: S. I. „Managementul documentelor”, „Resurse umane”, „Legislația”, „Contabilitatea” etc.)
<b>IV.</b>	<b>Interoperabilitate cu alte sisteme informatice interne ale IFpS</b>		Sisteme informatice de management a instituției (de exemplu: S. I. „Managementul documentelor”, „Resurse umane”, „Legislația”, „Contabilitatea” etc.)

În figura 4 este prezentată diagrama variantelor de utilizare a Portalului ”e-Contribuabil”.

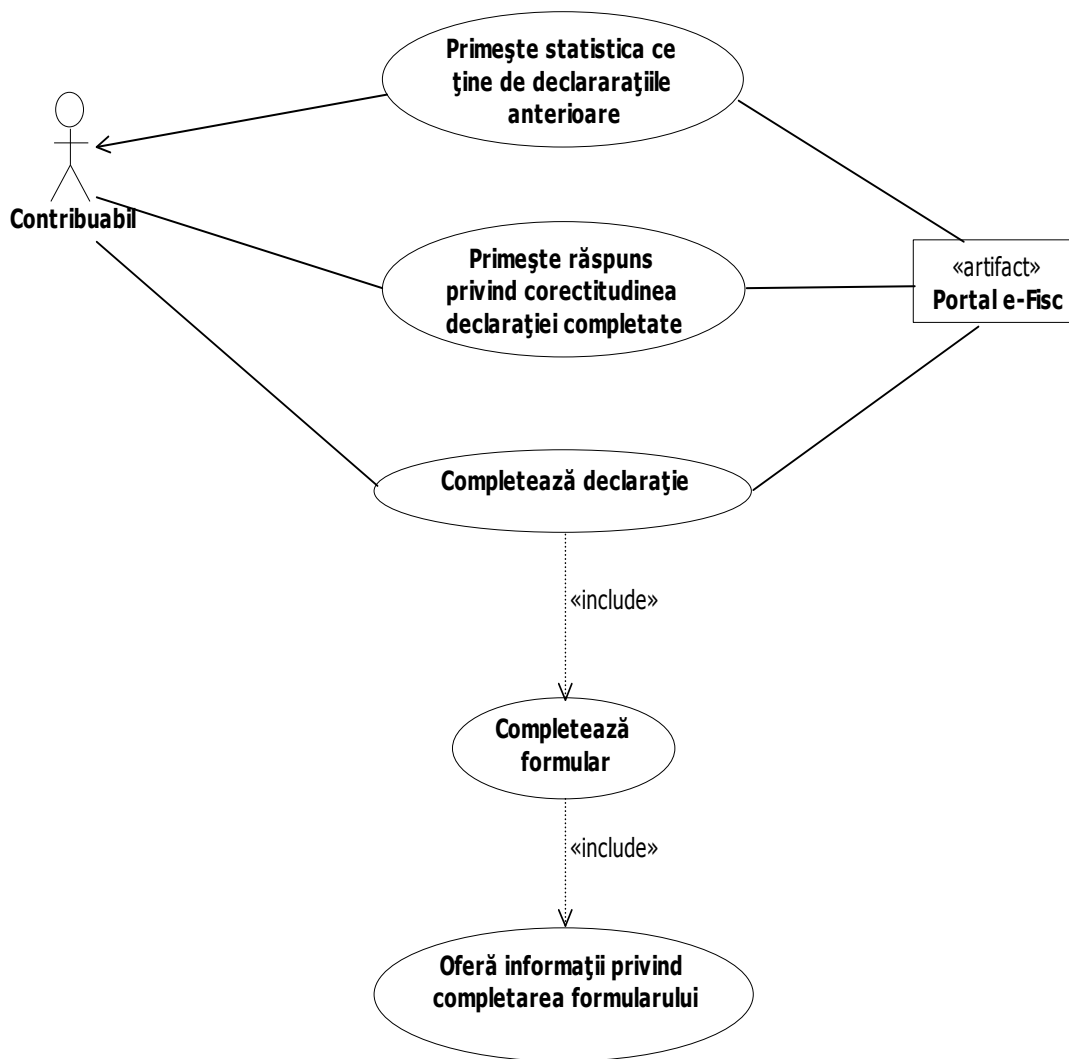


Fig.4. Diagrama Use Case. Completarea declarației utilizând Sistemul cu portal

Figura 5 reprezintă un scenariu de completare online a declarației. În acest caz Contribuabilul are la dispoziție o pagină Web ce conține câmpurile necesare tipului de declarație ales.



Fig.5. Diagrama secvențelor. Completarea declarației pe portalul ” e-Contribuabil”

Figura 6 reprezintă scenariul de încărcare a declarației deja completate. În acest caz declarația urmează a fi completată automat utilizând XML Schema descărcată în prealabil de pe portalul ”e-Contribuabil”.

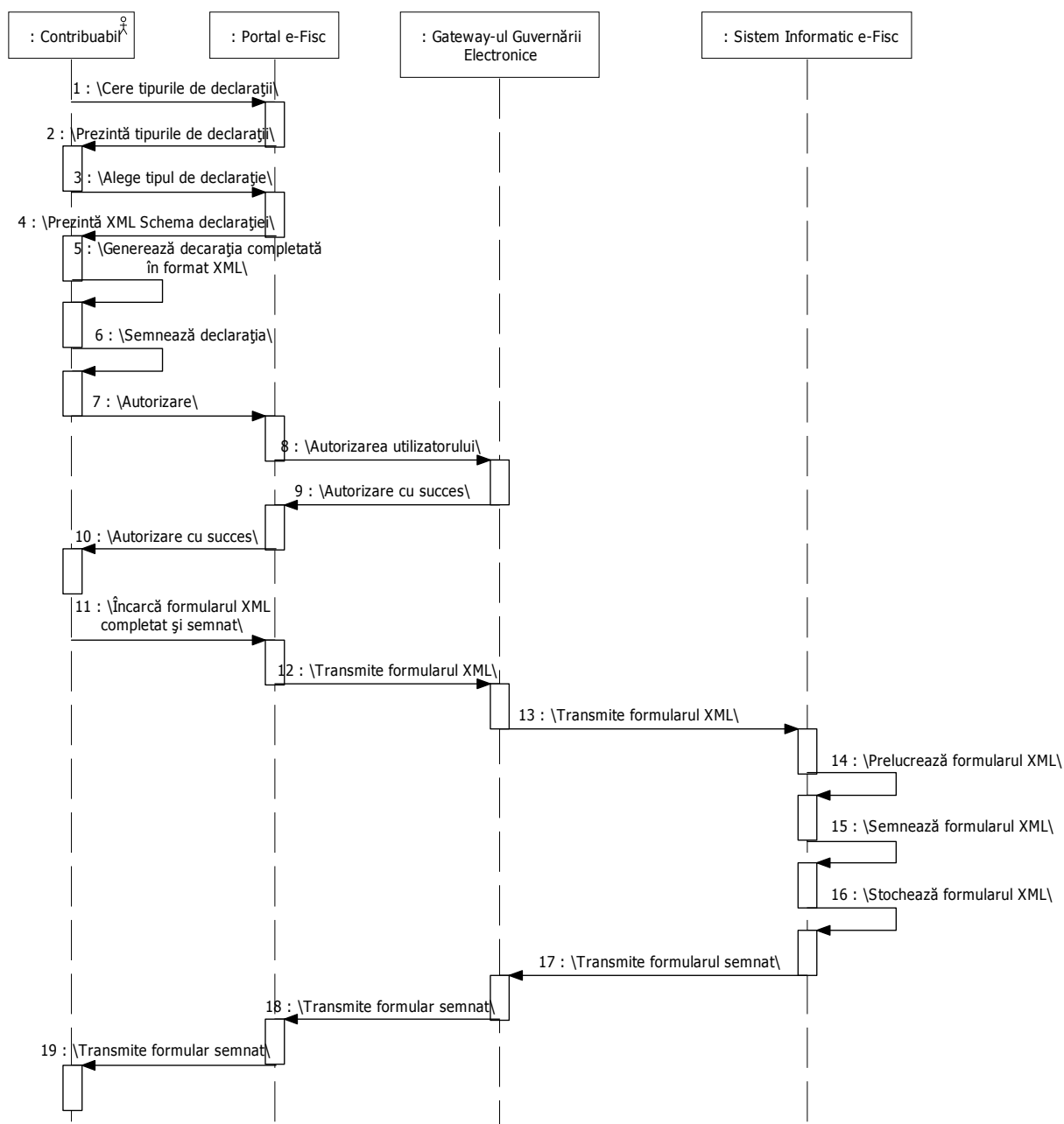


Fig.6. Diagrama secvențelor. Generarea declarației și încărcarea ei prin portalul ”e-Contribuabil”

Figura 7 ilustrează procesul de prezentare a declarației în cazul când IFpS, în baza informației fiscale de la persoanele juridice, completează declarația. În acest caz, contribuabilul primește declarația în format XML. Dacă formularul nu a suferit modificări, el este semnat și încărcat prin intermediul portalului. Dacă, însă, sunt necesare modificări, ele se introduc, după care, Contribuabilul semnează declarația modificată și o încarcă prin intermediul portalului.

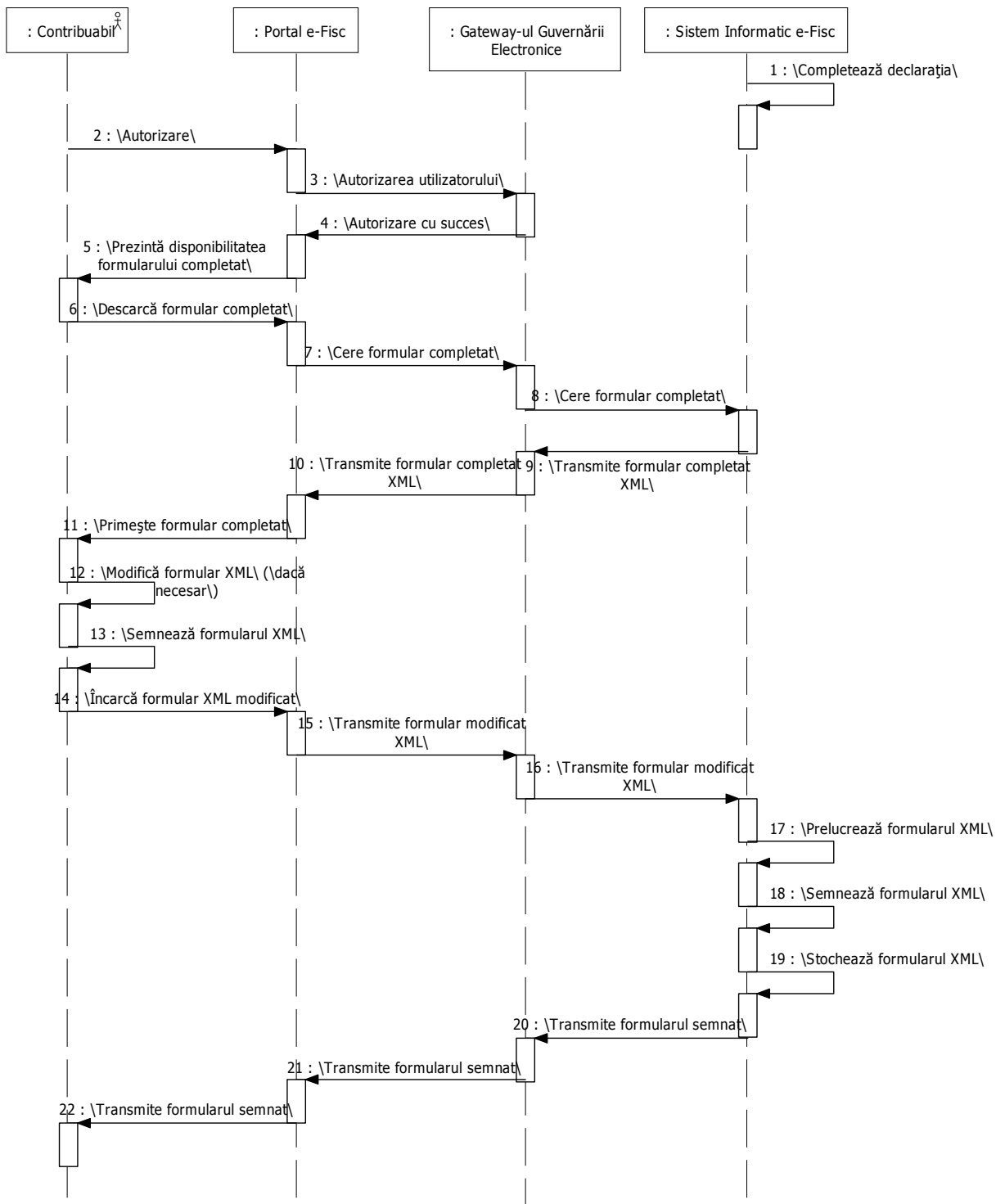


Fig.7. Diagrama secvențelor. Descărcarea, modificarea declarației și încărcarea ei prin portalul ” e-Contribuabil”

### 3.4 Bazele de Date

Cerințele față de Baza de Date includ:

- crearea, în conformitate cu structura funcțională, a documentelor inițiale și rezultative stabilite în cadrul Sistemului;

- compatibilitatea cu BD existente precum și cu eventualele modificări ce țin de dezvoltarea Sistemului;
- securitatea, la nivelul stabilit, a datelor și programelor de administrare a BD;
- receptivitatea la efectuarea procedurilor de corectare (modificare) a datelor;
- asigurarea accesului rapid al utilizatorilor în scopurile înmagazinării, modificării, extragerii și consultării datelor;
- BD - tip relațional;
- schema BD - normalizată la cel puțin Forma Normală 3;
- aplicarea tehnologiei OLAP sau a altor tehnologii similare pentru a obține analize online asupra datelor conținute în BD;
- acces la date a utilizatorilor finali și elaboratorilor aplicațiilor doar prin intermediul interpelărilor SQL;
- adăugarea, modificarea, distrugerea datelor din BD se efectuează doar de utilizatorii autorizați cu funcțiile respective;
- crearea mecanismelor ce depistează fraudele și accesul neautorizat la date;
- regimul „multi-utilizator” al BD;
- performanța de lucru cu BD - asigurarea în interval de până la 5 secunde între interpelare și primirea rezultatului;
- protejarea tranzacțiilor contra pierderilor de date (committed și rolled back);
- înștiințarea utilizatorului dacă tranzacția a avut loc cu succes sau nu;
- serverul de BD nu trebuie să aibă conexiuni cu rețeaua WAN;
- pentru administrarea serverului de BD în rețeaua LAN se va folosi SSLv3 sau VPN;
- asigurarea posibilității de rezervă (backup) și de recuperare (recovery) a datelor.

### 3.5 Sistemele de programare a aplicațiilor

Setul de programe trebuie să asigure:

- realizarea funcțiilor Sistemului, ce țin de crearea și administrarea Bazelor de date;
- realizarea funcțiilor de prestare servicii utilizatorilor prin intermediul rețelelor electronice LAN și WAN;
- realizarea conceptului de protejare a BD și de reglementare a accesului utilizatorilor la ele.

Programele aplicative vor conține mijloace de protejare contra utilizării neautorizate a lor.

Se presupune utilizarea următoarelor componente soft:

- mijloace de dezvoltare profesională a sistemelor;
- aplicații de colectare și raportare;
- aplicații evidentă și statistică;
- aplicații acces a persoanelor;
- analiză și menținere de date în sistem.

În programarea aplicațiilor sistemului se optează pentru:

- corectitudine;
- excluderea sensului dublu;
- complexitate;
- consistență;
- opțiuni de importanță sau de stabilitate;
- veracitate;
- modifiabilitate;
- trasabilitate.

Componentele soft urmează a fi stabilite definitiv în baza soluțiilor de proiect referitor la structura funcțională a sistemului, structura și volumul (în dinamică) BD și soluțiilor de proiect referitor la sistemul de securitate și protejare a datelor.

### **3.6 Sistemul tehnic de prelucrare și transportare a datelor**

#### **3.6.1 Sisteme de interconectare Internet / Intranet**

Specificările alese de interconectare Internet sau Intranet sunt următoarele:

- alinierea la Internet cu adoptarea WWW pentru sectorul public;
- adoptarea XML ca standard primar pentru integrarea datelor în sectorul public;
- soluție Web browser pentru interfața utilizator;
- schema de metadate pentru resursele informaționale ale-Guvernării;
- protocolul Internet IP v4, cu posibilități de trecere ulterioară la IP v6. ;
- standardele de mesaje SMTP/MIME pentru citirea mesajelor cu POP3;
- standard de mesaje securizate S/MIME v3. ;
- standard SOAP, UDDI și WDSL pentru serviciile Web;
- servicii DNS pentru rezoluția de nume Internet și Intranet;
- servicii FTP cu facilități de restart și recovery când se transferă fișiere de mari dimensiuni.

#### **3.6.2 Sisteme de transport date adiționale.**

Asigurarea tehnică a Sistemului informatic “e-Declarații” o constituie calculatoarele personale (PC) , inclusiv serverele tematice, mijloacele de imprimare, rețelele locale (LAN) și de aplicație largă (WAN).

Configurația minimală a calculatoarelor va fi determinată de sistemul de operare, volumul programelor aplicative și a bazelor de date, care urmează a fi precizat în procesul realizării etapelor de proiectare și implementare a Sistemului.

Sistemul integrat va fi instalat pe serverul rețelei locale a IFPS. Sistemele de asistență informațională a S.I. „e-Declarații” pentru utilizatorii din cadrul IFPS și subdiviziunilor subordonate se va realiza prin intermediul web-browserului.

Sistemul trebuie:

- să fie optimal, în limita normelor obiective de uzură, întru realizarea structurii funcționale și asigurarea extinderii ulterioare a Sistemului;
- să conțină componente prezente pe piața interioară a Republicii Moldova;
- să fie de o performanță comensurabilă cu cea a sistemelor de operare și programare;
- să fie flexibil în utilizarea mijloacelor disponibile destinate recepționării informației din surse externe (alte instituții publice);
- să asigure un nivel înalt de securitate în privința aplicațiilor și transportului de date.

#### **3.6.3 Securitatea datelor**

Securitatea informațională trebuie să fie asigurată printr-un sistem complex de măsuri juridico-normative, organizatorice și economice, cu utilizarea mijloacelor tehnologice, dispozitivelor software-hardware și metodelor criptografice de protecție a informației, orientat spre asigurarea nivelului necesar de integritate, confidențialitate și accesibilitate al resurselor informaționale.

Securitatea informațională trebuie să satisfacă următoarelor cerințe de bază:

- complexitate;
- concentrare pentru un anumit scop;
- neîntrerupere;
- fiabilitate;
- administrare centralizată.

Pericolele pentru securitatea informațională:

- obiecte ale pericolelor pentru securitatea informațională sînt resursele și infrastructura informațională;
- surse ale pericolelor pentru securitatea informațională pot fi infractorii, funcționarii de stat corupți, precum și utilizatorii de rea-credință;
- pericolele de bază pentru securitatea informațională sînt:
  - colectarea și utilizarea ilegală a informației;
  - încălcarea tehnologiei de prelucrare a informației;
  - implementarea în produsele software și hardware a componentelor, care realizează funcții neprevăzute în documentația de însoțire a acestor produse;
  - crearea și răspîndirea programelor, care afectează funcționarea normală a sistemelor informatice, rețelelor informaționale de telecomunicații, sistemelor de protecție a informației și altor sisteme informatizate;
  - nimicirea, deteriorarea, suprimarea radio-electronică sau distrugerea mijloacelor și sistemelor de prelucrare a informației, sistemelor de telecomunicații și comunicații;
  - influențarea asupra mijloacelor de protecție a sistemelor automatizate de prelucrare și transmitere a informației;
  - compromiterea cheilor și mijloacelor de protecție criptografică a informației;
  - sustragerea informației prin canale tehnice;
  - montarea ilegală a dispozitivelor electronice în mijloace tehnice de prelucrare, păstrare și transmitere a informației prin canalele de comunicații, precum și în încăperile de serviciu ale organelor puterii de stat pentru interceptarea informației;
  - nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau electronice;
  - interceptarea informației în rețelele de transmitere a datelor și pe liniile de comunicații, decodificarea acestei informații și impunerea informației false;
  - utilizarea tehnologiilor informaționale, a mijloacelor de protecție a informației, a mijloacelor de informatizare, de telecomunicații și comunicații necertificate, la crearea și dezvoltarea infrastructurii informaționale;
  - accesul neautorizat la resursele informaționale din băncile și bazele de date;
  - încălcarea restricțiilor legale privind răspîndirea informației;
  - atac asupra cheii / algoritm insuficient de puternic
  - analiza traficului;
  - acces neautorizat la postul de muncă;
  - acces neautorizat la rețea / resursele rețelei;
  - canale ascunse (covert channels);
  - spoofing de rețea;
  - viruși;
  - spam;
  - tunneling;
  - atacuri de tip DoS (denial of service) - întreruperea serviciilor;
  - repudiere;
- pericolele pentru securitatea informațională afectează:
  - confidențialitatea informației;
  - integritatea logică și integritatea fizică a informației;
  - funcționarea normală a infrastructurii informaționale;
- pericolele pentru securitatea informațională pot fi realizate prin următoarele moduri:
  - accesul neautorizat, ilegal sau nesancționat la resursele și infrastructura informațională;
  - influențarea fizică asupra componentelor infrastructurii informaționale;
  - organizarea ilegală a scurgerii informației prin diferite canale;
  - mituirea și/sau amenințarea personalului IFpS.

Sistemul de asigurare a securității informaționale trebuie să includă obligatoriu un șir de etape consecutive:

- determinarea profilurilor de protecție;
- categorisirea resurselor protejate;
- analiza riscurilor;
- elaborarea politicii de securitate;
- elaborarea arhitecturii de securitate;
- crearea și implementarea sistemului de securitate informațională;
- certificarea sistemului;
- organizarea studierii de către personal a metodelor și procedeele de contracarare a pericolelor pentru securitatea informațională.

Sistemul de asigurare a securității informaționale trebuie reexaminat și reajustat periodic sub aspecte juridic, organizatoric, tehnologic și economic. Utilizarea mecanismelor de asigurare a securității informaționale trebuie planificată la etapa proiectării sau modernizării sistemelor, resurselor și infrastructurii informaționale.

Sistemul de asigurare a securității informaționale trebuie să includă obligatoriu următoarele componente de bază:

- protecția informației și infrastructurii de mentenanță în cazul conectării la rețele externe;

- protecția informației în procesul interacțiunii dintre rețele;
- protecția fluxurilor de date;
- protecția service-lor sistemului;
- asigurarea integrității datelor;
- protecția antivirus;
- protecția anti-spam;
- asigurarea securității mediului software;
- autentificarea utilizatorilor;
- auditul.

Sistemul de securitate trebuie:

- să asigure accesul sancționat al utilizatorilor la BD, prin intermediul rețelelor LAN și WAN, cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiile fiecărui utilizator;
- să includă un sistem diferențiat de identificare a beneficiarilor și utilizatorilor, reieșind din rolurile acestora în realizarea funcțiilor Sistemului;
- să permită identificarea contribuabililor și a altor persoane fizice și juridice prin recurgerea la Registrele de Stat;
- să fie receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare, etc.);
- să fie receptiv la eventualele modificări ale drepturilor utilizatorilor referitor la elementele de structură ale BD accesibile lor;
- să includă mijloace de efectuare copii-rezerve pe diverse suporturi tehnice;
- să includă mijloace de protecție a datelor în cazuri de: dereglări de sistem, acces nesancționat, accidente tehnice;
- să includă mijloace de securitate a sistemului de programe;
- să includă mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor LAN și WAN;
- să includă mijloace de creare și consultare a arhivei speciale de date referitor la accesările (intențiile) nesancționate la date, indiferent de stadiul de prelucrare sau transportare a acestora.

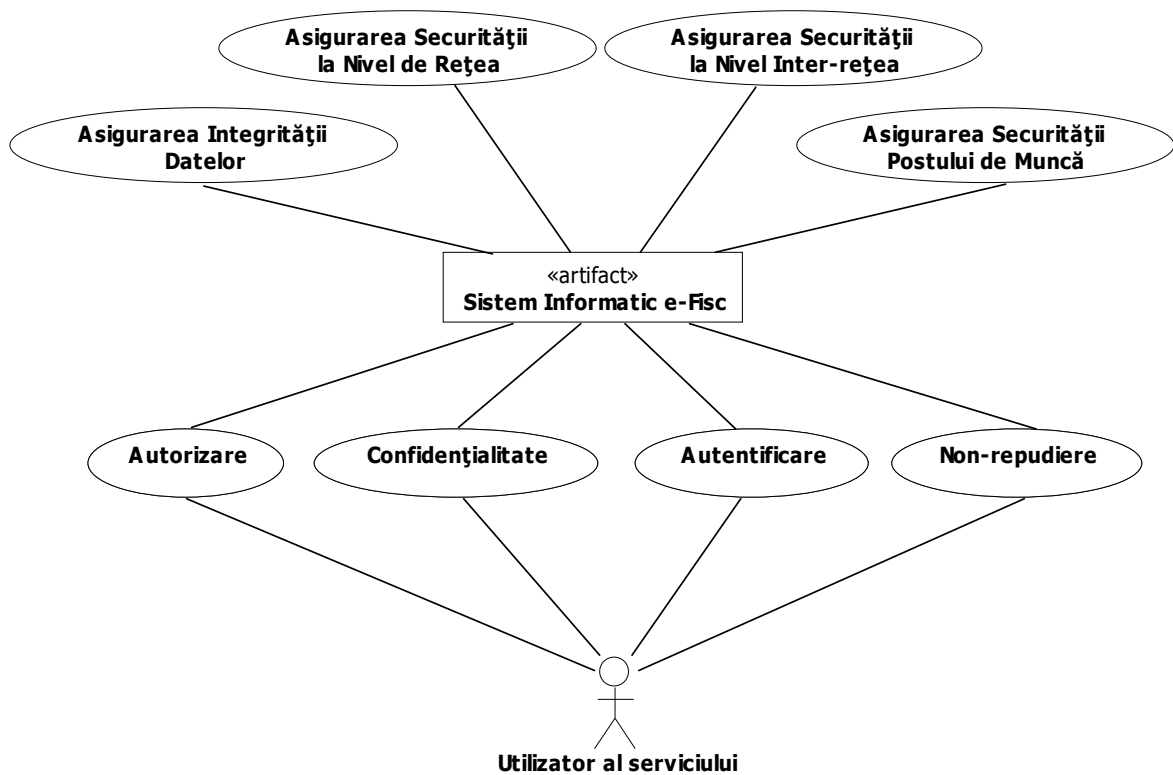


Fig.8 Securitatea utilizatorului serviciilor prestate de IFpS

Tipurile de informație:

- închisă (informație ce necesită un grad înalt de securitate, date personale, etc.)
- ce necesită un grad mediu de securitate
- publică (nu necesită mecanisme de criptare)
- în dependență de importanța informației vor fi alese mecanismele mai stricte sau mai puțin stricte de protecție a ei.

Securitate generală:

- IFpS își rezervă dreptul de a face auditul periodic al infrastructurii aplicațiilor sale pentru a se asigura de conformitatea cu standardele de securitate impuse;
- În cazul detecției unei breșe în securitate sistemul trebuie să aibă posibilitatea de deconectare parțială sau totală a funcționalităților.

Securitatea rețelei:

- trebuie create log-uri pentru toate încercările de acces atât reușite, cât și nereușite;
- rețeaua IFpS trebuie să fie separată de a altor întreprinderi;
- traficul trimis între serverul de baze de date și postul de muncă trebuie criptat;
- controlul resurselor trebuie să fie centralizat și să corespundă unei politici bine definite;
- accesul la resurse atât hardware, cât și software trebuie să fie divizat în dependență de competențele utilizatorilor.

Securitatea la nivel inter-rețea:

- rețeaua trebuie să fie protejată de exterior cu ajutorul unui instrument firewall și traficul dintre providerul de securitate și IFpS va fi protejat și autentificat prin tehnologii criptografice;

- controlul sesiunii și stării: Serverul trebuie să păstreze informația ce ține de starea sesiunii la trecerea de la o pagină la alta (de exemplu pentru a evita autentificarea repetată la deschiderea unei noi pagini);
- în sistem poate intra doar traficul autorizat ce este acceptat de politica de securitate impusă;
- tot traficul ce trece din sistem în exterior și invers trebuie să fie controlat de sistem.

#### Cerințe față de securitatea VPN:

- utilizarea VPN va fi controlată prin autentificare cu parole temporare, ca de exemplu, dispozitiv token sau un sistem de chei publice/private;
- nu este permis tunneling dual. Se permite doar o conexiune de rețea la un anumit moment dat;
- utilizatorii VPN care nu efectuează nici o activitate pentru 20 de minute sau mai mult vor fi deconectați automat. Utilizatorul se va autentifica din nou la reconectare. Ping sau alte procese artificiale nu vor fi utilizate pentru a menține conexiunea;
- conexiunea va dura nu mai mult de 24 de ore.

#### Securitatea Postului de Muncă:

- calculatorul trebuie să fie asigurat cu toate patch-urile la zi ale sistemului de operare;
- trebuie să existe informație privind timpul când trebuie să fie instalate patch-urile;
- administratorii trebuie să scaneze periodic posturile de muncă pentru a descoperi vulnerabilitățile;
- trebuie să existe un document ce reglementează lungimea minimă, regulile de generare și a perioadei de valabilitate a parolei;
- numele/parola conturilor locale nu poate fi folosită pentru crearea de noi conturi externe. (pentru a nu se divulga parolele la părți terțe);
- trebuie să existe o politică de creare, mentenanță și distrugere a conturilor;
- se utilizează pachetul anti-virus standard ales;
- actualizarea bazelor de date de viruși.

#### Standarde utilizate pentru elementele infrastructură de chei publice

- formatele certificatelor de chei publice: X509v3 (RFC2459);
- asigură posibilitatea obținerii certificatelor utilizând:
  - protocoalele de rețea: IKE, LDAPv3(RFC 3377);
  - suport extern: în format PKCS#7 sau pe token PKCS#11-compatibil;
- timpul de valabilitate a certificatelor nu trebuie să depășească 12 luni;
- autentificarea utilizatorilor se va face utilizând un token PKCS#11-compatibil;
- suport al CRL (Certificate Revocation Lists) și OCSP (Online Certificate Status Protocol);
- asigură primirea listelor de certificate revocate în format CRL utilizând LDAPv3;
- asigură suportul S/MIME (Secure / Multipurpose Internet Mail Extensions);
- asigură suportul SCEP(Simple Certificate Enrollment Protocol).

#### Web-Server:

- autentificarea (clientului și serverului):
  - se va produce în baza certificatelor serverului și a clientului în conformitate cu RFC 2069 Digest Access Authentication;
  - trebuie să existe un serviciu de setare a listei de certificate de încredere;
  - elementele de acces vor fi schimbate în fiecare 6-12 luni;
- autentificarea la nivel de aplicație:
  - se va produce la nivelul de aplicație a web-serverului;

- să conțină un mecanism de creare a parolelor ce vor fi greu de găsit prin criptanaliză;
- parolele transferate prin rețea vor fi în formă de coduri hash;
- sesiunea SSL trebuie să fie stabilită pentru toate adresările din partea clientului la resursa Web;
- datele trebuie să se păstreze în altă locație decât fișierele executabile;
- serverul trebuie să conțină mecanisme de rezervă (backup) și recuperare (recovery) a datelor;
  - web-serverul trebuie să fie instalat pe o platformă aparte de alte servere;
  - nu se admite plasarea pe aceeași platformă cu web-serverul a bazelor de date cu informație ce ține de procesul de lucru al IFpS;
  - administrarea web-serverului se va efectua prin intermediul consolei;
  - administrarea web-serverului se va efectua de pe un terminal la distanță prin rețea LAN prin intermediul consolei;
  - administrarea web-serverului se va efectua de pe un terminal la distanță prin rețea WAN prin intermediul consolei utilizând tunneling VPN;
  - schimbul de chei va fi efectuat conform protocolului IKE.

#### Module criptografice:

- trebuie să fie folosiți doar algoritmi standard (3DES, AES, RSA) pentru criptare;
- în cazul protecției informației închise, cheile pentru criptosistemele simetrice ar trebui să aibă o lungime ce ar asigura o protecție similară cu AES-cheie de 256 biți, sau 3DES-cheie de 168 biți;
  - în cazul protecției informației ce necesită un grad mediu de securitate, cheile pentru criptosistemele simetrice ar trebui să aibă o lungime ce ar asigura o protecție similară cu AES-cheie de 128 biți, 3DES-cheie de 128 biți;
  - în cazul protecției informației închise, cheile pentru criptosistemele asimetrice ar trebui să aibă o lungime ce ar asigura o protecție similară cu RSA-cheie de 2048 biți;
  - în cazul protecției informației ce necesită un grad mediu de securitate, cheile pentru criptosistemele asimetrice ar trebui să aibă o lungime ce ar asigura o protecție similară cu RSA-cheie de 1024 biți;
- modulele criptografice trebuie să corespundă FIPS PUB 140-2 (Requirements for Cryptographic Modules), cerințele concrete vor fi precizate pe parcursul etapei de proiectare;
- modulele criptografice trebuie să corespundă „Approved Key Establishment Techniques for FIPS PUB 140-2”;
- modulele criptografice trebuie să corespundă „Approved Protection Profiles for FIPS PUB 140-2”;
- modulele criptografice trebuie să corespundă „Approved Random Number Generators for FIPS PUB 140-2”;
- modulele criptografice trebuie să corespundă „Approved Security Functions for FIPS PUB 140-2”;
- hash-funcțiile folosite vor fi SHA, SHA-256, SHA-384;
- modulele criptografice ce implementează SHA trebuie să corespundă „FIPS PUB 180-2 Secure Hash Standard”;
- algoritmi și lungimea cheilor vor fi actualizați anual în dependență de nivelul tehnologiilor la zi;
- algoritmi vor fi aleși pentru utilizare doar în cazul în care ei au fost aprobați la nivel internațional ca fiind stabili și rezistenți la atacuri.

#### Cerințe față de baza de date de conturi (nume de utilizatori și parole):

- baza de date cu nume de utilizatori și parole trebuie să fie păstrată separat de codul programelor. Accesul la această bază de date trebuie să fie acordat doar persoanelor autorizate;

- mesajele de acreditare (credentials) vor fi păstrate pe un server de autentificare (server LDAP folosit pentru autentificarea utilizatorilor);

Parole:

- toate parolele la nivel de sistem (ex.: root, administrator NT, administrator de conturi) trebuie să fie schimbate cel puțin o dată în 3 luni;
- toate parolele la nivel de sistem trebuie administrate global într-o bază de date a parolelor;
- toate parolele la nivel de utilizator (ex.: email, Web, post de muncă) trebuie să fie schimbate cel puțin o dată în 6 luni. Perioada recomandată de valabilitate a parolelor este de 4 luni;
- contul utilizatorului care are privilegii la nivel de sistem acordat prin apartenență la un grup sau prin programe de tip „sudo” (superuser do) trebuie să aibă parolă diferită de alte conturi ale aceluiași utilizator;
- parolele NU trebuie să fie inserate în mesaje email sau în alte forme de comunicare electronică;
- colaboratorii IFpS nu au dreptul sub nici o formă să aducă la cunoștință loginul și parola nimănui, nici măcar familiei.

Accesul la distanță:

- accesul îndepărtat trebuie controlat strict. Conexiunea va fi stabilită doar cu utilizatori autorizați;
- persoanele conectate îndepărtat la rețea nu trebuie să aibă alte conexiuni la acel moment de timp. Conexiunea simultană cu altă rețea se admite doar în cazul în care utilizatorul este sigur de securitatea sa;
- routerele pentru linii dedicate ISDN configurate pentru acces la rețeaua IFpS trebuie să îndeplinească cerințele minime de autentificare a CHAP (Challenge Handshake Authentication Protocol);
- organizațiile sau persoanele care doresc să utilizeze o soluție nestandard de acces îndepărtat trebuie să obțină aprobarea de la administrator.

Securitatea fizică:

- echipamentul trebuie să fie plasat într-o încăpere protejată care este accesibilă doar personalului autorizat;
- echipamentul trebuie să fie plasat într-o încăpere protejată de unde electro-magnetice;
- IFpS are puterea de a autoriza persoanele cu drept de acces la echipament.

### **3.7 Statistica funcționării Sistemului**

Pe tot parcursul funcționării sistemul este necesar de prevăzut date și procese a evidenței de funcționare, care ar permite aprecierea funcționalității și prevederea unor măsuri de îmbunătățire. Este necesar de asigurat evidenta prin următoarele înregistrări:

- a proceselor;
- ale mesajelor și modul de informare;
- ale intervențiilor;
- ale evenimentelor și stărilor.

Datele de evidență vor fi supuse aprecierii prin rapoarte și mesaje informative, menite să elucideze situația sau starea de funcționare a sistemului.

Jurnalul de înregistrări trebuie să conțină:

- identificatorul utilizatorului;
- data, timpul și detalii ale evenimentelor cheie (ex.: intrare, ieșirea din sistem);

- identitatea terminalului de pe care se efectuează accesul;
- înregistrări ale tentativelor eşuate sau cu succes de acces la sistem;
- înregistrări ale schimbării configurației sistemului (ex.: schimbări sau tentative de schimbare a setărilor sistemului de securitate);
  - înregistrări ale utilizării conturilor cu privilegii (ex.: utilizarea contului supervizor, root, administrator);
  - înregistrări ale utilizării aplicațiilor;
  - înregistrări ale fișierelor accesate și modurilor de acces;
  - înregistrări ale adreselor de rețea și a protocoalelor;
  - alerte generate de sistemul de control al accesului;
  - înregistrări privind activarea și dezactivarea sistemelor de protecție (ex.: sisteme anti-virus, sisteme de prevenire/detectare a intruziunilor);
  - alerte de sistem (ex.: excepții de sistem, excepții ale sistemului jurnalului de înregistrări, alerte privind managementul de rețea);
  - înregistrări privind starea critică a proceselor.

### **3.8 Interoperabilitatea Sistemului cu alte sisteme informatice (Baze de Date), inclusiv Registrele de Stat**

Asigurarea interoperabilității Sistemului Informatic „e-Declarații” este un obiectiv menit să asigure funcționarea *completa și corectă* a sistemului. Concepția de e-Guvernare oferă mai multe soluții și modalități de ordin *organizațional, tehnologic și metodologic* de rezolvare a acestei probleme. Sarcina finală pentru a atinge obiectivul menționat constă în elaborarea componentelor sistemului.

Modul *organizațional* prevede modul de organizare a componentelor. De exemplu, autentificarea utilizatorului se pune în sarcina unei componente discrete Poarta(Gateway) în sistemul e-Declarații. Componenta va securiza și va asigura lucrul în sistemul local și în sistemele colaterale din cadrul e-Guvernare.

Modul *tehnologic* prevede, pentru acest caz, respectarea unui singur mod de reprezentare a datelor XML în tot sistemul integrat de e-Guvernare.

Modul *metodologic* constă, pentru acest caz, în implementarea modului de conectare la Internet prin proceduri de securizare unice, prin forme de identificare a utilizatorului prin card, forma de prezentare digitală a datelor, cum ar fi de exemplu, multimedia.

În procesul de proiectarea a componentelor se va ține cont de următoarele recomandări:

- platforma tehnică - soluție tehnică de Gateway;
- platforma software - sisteme operaționale și aplicații Microsoft;
- cadrul tehnologic - servicii Internet cu opțiuni de securizare;
- cerințe tehnice speciale - administrarea tranzacțiilor, autentificarea și înregistrarea utilizatorilor, securizarea datelor (ISO17999);
  - proceduri de lucru - Inspectoratul Fiscal de Stat, Ministerul Dezvoltării Informaționale; MAN și SIS;
  - standardizare - Internet IPv4(RFC), Date și securizare (ISO);
  - opțiuni speciale - multilingvism.

Modul de interacțiune între sistemele informaționale Registrul de Stat, Baza de Date (Trezoreria centrală și cele teritoriale), Casa Națională de asigurări și alte sisteme colaterale se vor stabili ca în Planul de Acțiuni.

### 3.9 Cerințe speciale referitor la „comportamentul” Sistemului cu contribuabilii și serviciile prestate acestora

Un obiectiv prioritar al Sistemul „e-Declarații” este accesul efectiv al utilizatorului la sistem și care impune diferite modalități de realizare de ordin *organizațional*, *tehnologic* și *metodologic*. Forma de bază a accesului public la sistem este declararea, notificarea și efectuarea de plăți a taxelor și impozitelor persoanelor fizice și juridice cu obligațiuni contribuabile față de stat. Sarcina finală pentru a atinge obiectivul menționat este finisarea componentelor.

Măsurile *organizaționale* prevăd divizarea sistemului în componente discrete, cum ar fi:

- componenta Portal - ce asigură prima treaptă de acces;
- componenta Gateway - ce asigură tranzacțiile cu sistemele colaterale.

Măsurile *tehnice* prevăd îmbinarea soluțiilor tehnice, cum ar fi:

- securizarea accesului - opțiune oferită de sistem;
- prezentarea datelor - opțiune, de asemenea, oferită prin diferite soluții și diferite nivele.

Măsurile *metodologice* impun alegerea unor anumite forme de comportament în dependență de utilizator(profil), cum ar fi:

- transparența în lucru - exclude cunoștințe despre modul de soluționare;
- infrastructura dinamică de portal - soluție e-Guvernare;
- excelență în soluție - creează o imagine psihologică ce predispune utilizatorul către soluția aleasă.

Măsurile de *proiectare* prevăd crearea sistemului în asemenea mod, încât să permită adaptarea continuă a mijloacelor oferite:

- dezvoltarea accesului - posibilitatea de a adăuga noi mijloace tehnice;
- scalabilitatea accesului - adaptarea performanței tehnice în dependență de necesități.

Măsurile de *sistem* includ măsuri prevăzute la etapa de integrare a soluțiilor ce permit:

- securizarea datelor - se asigură în fiecare din componente;
- interoperabilitatea Portalului - se asigură prin implementarea specificațiilor de date XML.

În procesul de proiectare a portalului se va ține cont de următoarele recomandări:

- platforma tehnică - soluție tehnică de portal;
- platforma software - sisteme operaționale și aplicații Microsoft;
- cadrul tehnologic - servicii Internet cu opțiuni de securizare;
- cerințe tehnice speciale - canale de comunicații multiple, dublarea funcționării unor componente, flexibilitate și extensibilitate pentru sesiuni de comunicații;
  - proceduri de lucru - Inspectoratul Fiscal de Stat, Ministerul Dezvoltării Informaționale, SIS;
- mod de informare - mediul de informare publică;
- standardizare - Internet IPv4 (RFC), Date și securizare (ISO);
- opțiuni speciale - multilingvism.

Interfața utilizatorului trebuie să fie completă funcțional, comodă și extensibilă. Interfața trebuie realizată în așa mod, încât să minimizeze greșelile utilizatorilor.

Cerințe:

- conținutul trebuie să se includă și să se reflecte corect într-o pagină cu aria de 640x480 pixeli;

- paginile să se redimensioneze dinamic pentru a folosi eficient ferestre mai mari ale browser-elor;
- paginile nu trebuie să supraîncarce font-urile proprii în detrimentul celor ale utilizatorului. Utilizatorul trebuie să aibă posibilitatea de a ajusta dimensiunea și fontul prin setările standarde ale browser-ului;
- toate paginile trebuie să se încarce complet (inclusiv grafica) în 5 secunde la viteză de conexiune de 56 kbps;
- utilizarea butonului „Back” nu trebuie să aibă ca rezultat erori;
- pot fi folosite culori diferite pentru link-uri, dar setul de culori (active, vizitate, nevizitate) trebuie să fie același pe toate paginile;
- paginile Web nu trebuie să producă ferestre „pop-up”;
- toate imaginile trebuie să fie descrise;
- statutul tranzacțiilor incomplete trebuie să fie salvat și interfața trebuie să permită recuperarea acestora;
- interfața trebuie să vizualizeze transferul de informații (declarații, etc.) între utilizator și server.

Procesul de proiectare se va efectua în corespundere cu standardele de calitate a sistemelor software, soluții și instrumente tehnologice ( Anexa 3.). La cerințele menționate mai sus se adaugă și cerința *calitățile de acces* care necesită formalizare în oferte.

### **3.10 Cerințe speciale referitor la gradul de „deschidere” a Sistemului către portalul central e-Guvernare și Gateway Guvernului**

Sistemul „e-Declarații” este preconizat să funcționeze integrat cu sistemul e-Guvernare, prin intermediul porții de acces a Guvernului (GG- Gateway Guvernamental ). În acest context sunt necesare reglementări și proceduri de ordin organizațional și tehnologic, care să asigure funcționarea deplină și stabilă a întregului sistem.

Sistemul e-Guvernare asigură un rol de centralizare a sistemelor informaționale existente locale. Drept mediu de interconectare va servi mediul Internet , care include soluții tehnologice aprobate. Sistemul Central va pune la dispoziția utilizatorilor:

- interconectare cu mediul Intranet Guvernamental Securizat ( S/MIME și conexiuni TLS/SSL de cel puțin 128 biți);
- interacțiunea serviciilor publice ( Portal Guvernamental, WWW, DNS,FTP,IPv4);
- servicii de autentificare, asigurând accesul generalizat la resurse informaționale;
- securitatea și protecția informațiilor în conformitate cu profilul utilizatorului;
- formate speciale pentru schimburi de date (cerințe XML,XSL);
- funcții de management.

Sistemul „e-Declarații” asigură funcționarea internă completă și un rol de „colaborare” funcțională cu sistemul e-Guvernare. Sistemul e-Declarații pune la dispoziția utilizatorilor:

- mediu de Internet sau mediu de Intranet Departamental Securizat cu interconectare la sistemul e-Guvernare (S/MIME și conexiuni TLS/SSL de cel puțin 128 biți);
- interacțiunea serviciilor publice (Portal e-Declarații) și interconectarea cu Portalul e-Guvernare (WWW,DNS,FTP,IPv4);
- servicii de autentificare locală și centralizată;
- formate speciale pentru schimburi de date (cerințe XML,XSL);
- funcții de management;
- funcții publice de prestare a serviciilor;
- funcții interne de gestiune și prelucrare a datelor.

Gradul de „deschidere” a Sistemului „e-Declarații” către sistemul integrat e-Guvernare este determinat de prezența funcțiilor comune din lista prezentată mai sus. Funcțiile interne de gestiune și

prelucrare a datelor în sistem nu sunt incluse în această listă. Deschiderea sistemului Local către cel Central asigură o funcționare *stabilă* a sistemului integrat.

Pentru ca Sistemul informatic „e-Declarații” să fie perfect *integrat, deplin și stabil* se cere delimitarea serviciilor interne de cele publice, folosind măsuri eficiente de securizare. Se vor stabili și măsuri *procedurale* a „deschiderii” la etapa de implementare a sistemelor.

### 3.11 Cadrul normativ – juridic

Soluțiile de proiect ale Sistemului informatic “e-Declarații”, instrucțiunile și normele de exploatare a lui necesită suport juridic.

Cadrul normativ-juridic al S. I. „e-Declarații” se va reglementa de legislația internă a Republicii Moldova și tratatele internaționale la care Republica Moldova este parte.

La crearea, utilizarea și menținerea în funcțiune a Sistemului trebuie să se țină cont de prevederile următoarelor acte juridico-normative:

- Constituția Republicii Moldova;
- Decretul Președintelui Republicii Moldova nr.1743-III din 19.03.2004 privind edificarea societății informaționale în Republica Moldova;
- Legea nr.780-XV din 27.12.2001 privind actele legislative;
- Legea nr.317-XV din 18.07.2003 privind actele normative ale Guvernului și ale altor autorități ale administrației publice centrale și locale;
- Legea nr.467-XV din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr.264 din 15.07.2004 cu privire la documentul electronic și semnătura digitală;
- Legea nr.595-XIV din 24.09.1999 privind tratatele internaționale ale Republicii Moldova;
- Legea nr.284-XV din 22.07.2004 privind comerțul electronic;
- Legea nr.1069-XIV din 22.06.2000 cu privire la informatică;
- Legea nr.982-XIV din 11.05.2000 privind accesul la informație;
- Tratatelor internaționale ce țin de drepturile omului la care Republica Moldova este parte;
- Hotărârea Guvernului nr.255 din 09.03.2005 privind Strategia Națională de edificare a societății informaționale – "Moldova electronică";
- Hotărârea Guvernului nr.320 din 28.03.2006 pentru aprobarea Regulamentului privind modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice;
- Hotărârea Guvernului nr.632 din 08.06.2004 despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova;
- Hotărârea Guvernului nr.272 din 06.03.2002 despre măsurile privind crearea sistemului informațional automatizat "Registrul de stat al unităților de drept";
- Hotărârea Guvernului nr.333 din 18.03.2002 pentru aprobarea Concepției sistemului informațional automatizat "Registrul de stat al populației" și Regulamentului cu privire la Registrul de stat al populației;
- Hotărârea Guvernului nr.618 din 05.10.1993 pentru aprobarea Regulilor de întocmire a documentelor organizatorice și de dispoziție și Instrucțiunii-tip cu privire la ținerea lucrărilor de secretariat în organele administrației publice centrale de specialitate și ale autoadministrării locale ale Republicii Moldova;
- Hotărârea Guvernului nr.115 din 28.02.1996 pentru aprobarea Instrucțiunilor cu privire la ținerea lucrărilor de secretariat în organele administrației publice locale ale Republicii Moldova;
- regulamentele și normele interne de reglementare a activităților organelor fiscale;
- reglementarea relațiilor și acțiunilor interdepartamentale ce țin de determinarea ordinii de implementare și funcționare a circulației electronice a documentelor, de

ținere a lucrărilor de secretariat, cu aplicarea tehnologiei informaționale de performanță în cadrul autorităților administrației publice, se vor aproba la necesitate de către Guvern.

În procesul de creare, implementare și exploatare a Sistemului urmează a fi reglementate din punct de vedere normativ și juridic următoarele activități și comportamente:

- lista, volumul, termenele și succesiunea efectuării lucrărilor;
- selectarea, instalarea și respectarea condițiilor de exploatare a mijloacelor informatice;
- respectarea condițiilor de implementare, exploatare și dezvoltare a Sistemului;
- asistența materială pe etape de proiectare, implementare și dezvoltare a Sistemului.

Obligațiunile și responsabilitățile asumate de către părțile angajate vor fi stipulate, având efect normativ-juridic egal, în următoarele categorii de documente:

- contracte;
- procese - verbale, acte, programe de lucru și alte documente semnate de părți;
- standarde, instrucțiuni, directive ale organelor de resort și alte documente care reglementează activitățile organelor fiscale;
- standarde, norme și alte documente care reglementează activitățile de proiectare și implementare a sistemelor informatice;
- documente de proiect semnate de părți, inclusiv instrucțiuni ale schemelor XML a dărilor de seamă fiscale.

### 3.12 Parametrii de exploatare ulterioară a Sistemului

Exploatarea ulterioară, întreținerea și dezvoltarea Sistemului se va efectua conform sarcinilor și funcțiilor enumerate în prezentul document, care vor fi precizate pe parcursul elaborării și implementării Sistemului.

Soluțiile de proiect trebuie să garanteze unii parametri de exploatare ulterioară:

- viteza înalta de prelucrare a tranzacțiilor în regim accesări simultane la BD a utilizatorilor, exprimata prin timpul minimal de reacționare la interpelare;
- simplitatea de însușire și funcționare, care presupune:
  - planificarea ecranelor, care asigura apropierea maximala către modelele reale de lucru;
  - planificarea fișierelor (textelor) de ajutor;
  - accesibilitatea documentației;
  - minimizarea situațiilor neprelucrabile;
- siguranța în exploatare care presupune:
  - planificarea corectă a evenimentelor și situațiilor, care pot conduce la distrugerea programelor și datelor;
  - excluderea variantelor blocării Sistemului;
  - asigurarea funcționării în situații de accidente.

### 3.13 Cerințe suplimentare

**Arhiva** se referă la sistemul informatic și se creează în scopul eliminării din BD a datelor neactuale.

Periodicitatea arhivării și anularii informației este determinata prin regulamentele IFpS, iar în lipsa acestora – de către administratorii BD.

Mijloacele de administrare a arhivei trebuie să:

- permită schimbul reciproc de date cu BD;
- asigure accesul administratorului BD și efectuarea procedurilor de selectare și consultare a datelor;
- asiste securitatea și reglementarea accesului identic la BD;

Absolut orice funcționar trebuie să aibă cutie email, cu numele propriu și alias la funcție, dacă e funcție importantă. Alias-ul automat trece altei persoane la necesitate (schimbări de cadre).

## **4. Ofertă**

### **4.1 Introducere**

**Denumirea: Sistem informatic cu Portal „e-Declarații”**

**Domeniu:** Colectarea, depozitarea și prelucrarea declarațiilor fiscale, folosind mijloace electronice în regim „on-line” prin intermediul Internet /Intranet.

**Obiectul de implementare :** Inspectoratul Fiscal principal de Stat

### **4.2 Bazele pentru elaborare**

Prezentul Caiet de sarcini este elaborat în cadrul proiectului Programul Națiunilor Unite pentru Dezvoltare în Moldova (PNUD) și a Guvernului „Implementarea componentei e-Guvernare a Strategiei Naționale de edificare a Societății Informaționale din Republica Moldova”. Caietul de sarcini a fost discutat în cadrul grupului tehnic de consultanță a proiectului și coordonat cu Inspectoratul Fiscal principal de Stat, Ministerul Dezvoltării Informaționale și Centrul de Comunicații Speciale. Documentul este destinat pentru organizarea unei licitații pentru alegerea companiei, care va elabora și implementa Sistemul informatic cu Portal „e-Declarații”.

### **4.3 Obiective**

Sistemul informatic cu Portal „e-Declarații” este preconizat pentru colectarea, depozitarea și prelucrarea datelor ce țin de declarațiile fiscale ale persoanelor fizice și juridice din Republica Moldova. Aceste responsabilități sunt indicate în Codul Fiscal și în alte regulamente aferente. Sistemul informatic în varianta propusă respectă principiile de bază și include în sine componentele prevăzute în concepția de implementare e-Guvernare.

Beneficiar: Inspectoratul Fiscal principal de Stat, Ministerul de Finanțe. (<http://www.fisc.md>)

### **4.4 Cerințe fața de Sistem.**

#### **4.4.1 Caracteristicile funcționale**

B.1. *Înregistrarea* declarațiilor fiscale în regim on-line, utilizând mediul și mijloacele Internet, prin proiectare de e-Portal, inclus în Sistem informatic.

Condiții inițiale:

- portalul va permite înregistrarea a 6-10 mln de declarații fiscale anual cu un volum aproximativ de 100 Mgb;
- ofertanții vor proiecta Portalul și mijloacele de acordare pentru o reacție minimă client-sistema de 0-30s;

B.2. Configurarea și urmărirea fluxului tuturor categoriilor de declarații fiscale.

B.3. *Interoperabilitatea* cu sistemul existent al IFpS, Trezoreria de Stat și alte sisteme informatice, folosind instrumente de redactare și prezentare a datelor în format XML.

B4. Crearea automatizată a *procedurilor de colectare* on-line a declarațiilor fiscale în baza formularelor aprobate de declarații.

B.5. Diferite *nivele de acces* (nivele diferențiate de acces la operare: completare, prelucrare, înregistrare, verificare)

B.6. Sistem de *raportare* preventivă flexibil după diferite criterii: tip de documente, nume de persoane, termen de prezentare.

B.7. *Arhivare*. Sistemul de colectare a declarațiilor fiscale *va* efectua regulamentul și operativ arhivarea datelor în Sistemul informatic existent, care va fi exploatat în continuare ca platformă de bază a IFpS.

B.8. *Cautarea* documentelor după diferite criterii: - număr înregistrare, data depunerii, numele petentului, adresa, tipul de declarație, cuvânt-cheie, etc.

B9. Ajustarea *mijloacelor de conexiune* la Portal prin Internet (e-Guvernare).

B10. *Functii specifice* de Portal :

- asistență informativă - ajutor, școlarizare, informare ;
- liste de prezență - contacte, adrese de referință;
- opțiuni de interacțiune cu Sistemul;
- evidență și adaptare a utilizatorilor și a profilurilor;
- interfețe cu mijloacele de securitate și autentificare de acces;
- management de conținut;
- instrumente de creare a formularelor pentru prezentarea documentelor;
- mecanisme de mesaje, care rutează documentele spre destinatar, convertindu-le în formatul sistemelor de destinație;
- mecanism unitar de reglare, care stabilește regulile de procesare a documentelor;
- interfață de lucru;.
- aplicație de management a conținutului;
- structură unitară pentru dezvoltarea, administrarea și mentenanța serviciilor;
- alte funcții.

#### **4.4.2 Cerințe de fiabilitate**

C1. Ofertanții *vor* proiecta Portalul și mijloacele de prestare servicii pentru un regim de funcționare 24ore/ 7 zile;

C2. Portalul *va* asigura prezentarea datelor de declarații fiscale la Inspectoratele Fiscale principale de Stat, folosind mijloace electronice, pe o perioadă de 3 ani (până la sfârșitul anului calendaristic 2009).

#### **4.4.3 Condiții de exploatare**

D1. Proiectul *va* fi modular. Extensiile ulterioare nu trebuie să implice reorganizarea datelor din Sistem și / sau costuri suplimentare semnificative, și nu trebuie să afecteze funcționalitatea și performanța Sistemului.

#### **4.4.4 Componenta și parametrii resurselor tehnice**

E1. Oferta *va* prevedea folosirea echipamentului tehnic, care există la moment în IFpS în calitate de:

- Portal Server – server IBM OpenPower 720 cu RISC procesor și sistemul operațional SUSE Linux Server 9;
- Server Operațional - server de colectare și prelucrare a declarațiilor fiscale în baza de IBM OpenPower 720 cu RISC procesor, sistemul operațional SUSE Linux Server 9 și Sistemul de Gestionare a Bazelor de Date Informix ver. 10.0 licențiată pe procesoare;

E2 Oferta *va* prevede recomandări de înzestrare suplimentară cu echipament tehnic.

#### **4.4.5 Compatibilitate informațională și de Sistem**

F1. Proiectul *va* include mijloace de acordare cu componente care *exista recent* sau *vor fi prevazute* pe viitor in cadrul Sistemului informatic :

- Firewall, mijloace de prevenire a accesului neautorizat in rețea;
- server de autentificare a utilizatorilor in rețea (Gateway) cu protecție SMTP și detecție SPAM.
- server de certificare și infrastructura de key publice (certIFICATE X509v3, Directory Server LDAP / X.500 );
- sistemul de detectare a intrușilor in traficul TCP/IP;
- WEB Mail server pentru a primi de la sau transmite către contribuabili date prin e-mail;
- server Antivirus pentru a proteja punctele de access ale sistemelor;
- server DNS pentru Name Server și Resolver (LDAP v3 /ITU X.500);

F2. Oferta *va* prevede utilizarea mediului Internet /Intranet pentru a folosi serviciile de Portal. Se recomandă de inclus servicii de e-business și aplicații de voce (VoIP-voice over IP, VPN – virtual private network, QoS –quality of service și altele) *va* fi un avantaj.

#### **4.4.6 Marcare și ambalaj;**

Oferta *va* include condiții, ca toate echipamentele și produsele soft livrate vor fi însoțite de marci și indici ai producătorului în conformitate cu legile în vigoare în Republica Moldova.

#### **4.4.7 Transportare și păstrare;**

Oferta *va* prevede livrare CIP la locația IFpS Chisinau, Moldova.

#### **4.4.8 Cerințe speciale.**

Oferta *va* include măsuri speciale ce se referă la :

- instalare;
- scolarizarea operatorilor;
- testare a soluției;
- servicii adăugătoare de mentenanță.

#### **4.4.9 Documente de însoțire**

Oferta *va* include livrarea setului de documente, necesare pentru instalare, implementare și exploatare ulterioară a Sistemului.

#### **4.4.10 Stadii de elaborare.**

Ofertanții *vor* proiecta Portalul și mijloacele de acordare pentru implementare în decurs 2 luni de la data semnării contractului.

#### **4.4.11 Ordinea de predare-primire**

Finalizarea lucrărilor “on-key” se face prin act de primire-predare.

## Termeni și acronime

<b>Blog</b>	- pagină personală, în care funcționarul își poate expune părerea zi de zi asupra unor probleme în stat, societate. Provine de la „Web Log”.
<b>BD</b>	- Baze de Date;
<b>LAN</b>	- mediu de rețea locală ( Local Area Network);
<b>PC</b>	- calculator personal pentru automatizarea proceselor de vizualizare, colectare și prelucrare a datelor;
<b>Sisteme colaterale</b>	- sisteme informatice cu orientare similară cu Sistemul informatic „e-Declarații”;
<b>WAN</b>	- mediu de rețea, care presupune componente distanțate semnificativ ( Wide Area Network)

**Lista tipurilor de documente admisibile în IFpS.**

Tipul documentului	<i>Denumirea documentului</i>	Tipul pachetului *)	Prioritatea prelucrării
<b>DS</b>	Document de plată trezorerial la bugetul de stat	S	0
<b>DL</b>	Document de plată trezorerial la bugetul local	L	0
<b>REG</b>	Registru sumelor încasate în numerar de IFS și primării	N	0
<b>KIT</b>	Chitanțieră de plată	N	0
<b>DFISC</b>	Decizie de stingere a obligațiunilor fiscale	C	1
<b>F115</b>	Modificările obligațiunilor fiscale	C	1
<b>ACT</b>	Actul de control	C	1
<b>ACZ</b>	Calculul accizelor	C	1
<b>AR</b>	Formular cu privire la reflectarea în fișa personală a sumelor acceptate la restituire în baza deciziei	C	1
<b>TVA02</b>	Declarația privind taxa pe valoarea adăugată	C	1
<b>RIS</b>	Darea de seamă cu privire la impozitul pe venit reținut din plățile salariale	C	1
<b>RIA</b>	Darea de seamă cu privire la impozitul pe venit reținut din sursele de venit altele decât plățile salariale.	C	1
<b>CNOTAR</b>	Calculul impozitului pe venit al notarului privat	C	1
<b>CAD</b>	Cerere de anulare a documentului	A	1
<b>CIR</b>	Cerere de înscriere repetată a documentului	W	1
<b>FUNJ03</b>	Calculul impozitului funciar persoane juridice	C	2
<b>BIJ</b>	Calculul impozitului pe bunurile imobiliare ale persoanelor juridice	C	2
<b>BIF</b>	Calculul impozitului pe bunurile imobiliare ale persoanelor fizice care desfășoară activitatea de întreprinzător	C	2
<b>BIPF</b>	Darea de seamă privind sumele impozitului funciar și pe bunurile imobiliare calculate persoanelor fizice (cetățeni) și gospodăriilor țărănești (de fermier)	C	2
<b>CNAM</b>	Raport privind calcularea și transferul primelor de asigurare obligatorie de asistență medicală	C	2
<b>TAT</b>	Darea de seamă pe taxa pentru amenajarea teritoriului	C	2
<b>TLL</b>	Darea de seamă pe taxa pentru dreptul de a organiza licitații și loterii	C	2
<b>TH</b>	Darea de seamă pe taxa hotelieră	C	2
<b>TR</b>	Darea de seamă pe taxa pentru amplasarea publicității (reclamei)	C	2
<b>TAS</b>	Darea de seamă pe taxa pentru dreptul de a aplica simbolică locală	C	2

<b>TAUC</b>	Darea de seamă pe taxa pentru amplasarea unităților comerciale	C	2
<b>TP</b>	Darea de seamă pe taxa de piață	C	2
<b>TRA</b>	Darea de seamă pe taxa pentru parcare autovehiculelor	C	2
<b>TB</b>	Darea de seamă pe taxa balneară	C	2
<b>TPC</b>	Darea de seamă pe taxa de la posesorii de câini	C	2
<b>TTF</b>	Darea de seamă pe taxa pentru trecerea frontierei de stat	C	2
<b>TCZV</b>	Darea de seamă pe taxa pentru dreptul de a vinde în zona vamală	C	2
<b>TTC</b>	Darea de seamă pe taxa pentru dreptul de a presta servicii de transportare a călătorilor	C	2
<b>IP</b>	Darea de seamă pe impozitul privat	C	2
<b>LTA</b>	Darea de seamă privind calculul sumei taxei de eliberare a licențelor pentru activități în transportul auto	C	2
<b>ATRI</b>	Darea de seamă privind calculul sumei taxei de eliberare a autorizațiilor pentru transporturi rutiere internaționale	C	2
<b>AVSM</b>	Darea de seamă privind calculul sumei taxei de eliberare a autorizațiilor pentru circulația vehiculelor cu sarcină masivă pe osie și cu gabarite care depășesc limitele admise	C	2
<b>AZP</b>	Darea de seamă privind calculul sumei taxei de eliberare a autorizațiilor pentru lucrări în zona de protecție a drumurilor	C	2
<b>TA</b>	Darea de seamă a taxei pentru apă	C	2
<b>TEG</b>	Darea de seamă pentru dreptul de a efectua explorări geologice	C	2
<b>TPG</b>	Darea de seamă a taxei pentru dreptul de a efectua prospecțiuni geologice	C	2
<b>TMU</b>	Darea de seamă a taxei pentru dreptul de a extrage minerale utile	C	2
<b>TSE</b>	Darea de seamă a taxei pentru dreptul de a folosi subsolul pentru construcții subterane, altele decât cele destinate extracției mineralelor utile	C	2
<b>TSC</b>	Darea de seamă a taxei pentru dreptul de a folosi subsolul în scopul exploatării construcțiilor subterane	C	2
<b>TL</b>	Darea de seamă a taxei pentru lemnul eliberat pe picior (venitul silvic)	C	2
<b>TGL</b>	Darea de seamă privind calculul sumei taxei pentru comercializarea gazului lichefiat și gazelor naturale destinate utilizării în calitate de combustibil pentru unitățile de transport auto	C	2
<b>TAOR</b>	Darea de seamă privind calculul sumei taxei de eliberare a autorizațiilor pentru amplasarea de obiective pentru prestarea serviciilor rutiere în zona de protecție a drumurilor	C	2
<b>TFD</b>	Darea de seamă privind calculul sumei taxei de folosire a drumurilor percepută de la posesorii de vehicule înmatriculate în Republica Moldova	C	2

<b>V2000</b>	Declarația cu privire la impozitul pe venit a persoanei, ce practică activitatea de întreprinzător (Forma VEN aprobată prin Instrucțiunea Serviciului Fiscal de Stat nr.3 din 29 ianuarie 2001)	C	3
<b>CET</b>	Declarația persoanei fizice cu privire la impozitul pe venit	C	3
<b>TVAFACT</b>	Anexa privind facturile TVA primite în perioada fiscală	C	4
<b>IAL01</b>	Notă de informare privind plățile salariale și alte plăți efectuate de către patron în folosul angajaților și privind impozitul pe venit reținute din aceste plăți	C	5
<b>IAS01</b>	Notă de informare privind plățile rezidenților din sursele de venit, altele decât plățile salariale, și privind impozitul pe venit reținut din aceste plăți	C	5
<b>INR01</b>	Notă de informare privind impozitul reținut din sursele de venit, altele decât plățile salariale, achitate persoanelor nerezidente	C	5
<b>VEP</b>	Notă de informare privind veniturile sub formă de dobândă și royalty achitate în folosul persoanelor fizice rezidente în vîrstă de 60 ani și mai mult	C	5
<b>NOT</b>	Notă de informare privind tranzacțiile cu activele de capital autentificate notarial, efectuate de către persoanele juridice și fizice	C	5

\*) - Tipul pachetelor

<b>Tipul pachetului</b>	<b>Destinația pachetului</b>
<b>C</b>	Pachete ce conțin documente fiscale, cu excepția celor de plată.
<b>S</b>	Pachete electronice primite de la Trezoreria de Stat
<b>L</b>	Pachete electronice primite de la Trezoreriile teritoriale
<b>N</b>	Pachete ce conțin documente de plată în numerar
<b>F</b>	Pachete electronice primite de la Casa Națională de Asigurări Sociale
<b>W</b>	Pachete ce conțin cereri de înscriere repetată a documentelor fiscale
<b>A</b>	Pachete ce conțin cereri de anulare documentelor fiscale

### **Pericolele pentru securitatea informațională**

- a) Obiecte ale pericolelor pentru securitatea informațională sînt resursele și infrastructura informațională.
- b) Surse ale pericolelor pentru securitatea informațională pot fi infractorii, funcționarii de stat corupți, precum și utilizatorii de rea-credință.
- c) Pericolele de bază pentru securitatea informațională sînt:
  - colectarea și utilizarea ilegală a informației;
  - încălcarea tehnologiei de prelucrare a informației;
  - implementarea în produsele software și hardware a componentelor, care realizează funcții neprevăzute în documentația de însoțire a acestor produse;
  - crearea și răspîndirea programelor, care afectează funcționarea normală a sistemelor informatice, rețelelor informaționale de telecomunicații, sistemelor de protecție a informației și altor sisteme informatizate;
  - nimicirea, deteriorarea, suprimarea radio-electronică sau distrugerea mijloacelor și sistemelor de prelucrare a informației, sistemelor de telecomunicații și comunicații;
  - influențarea asupra sistemelor de protecție a sistemelor automatizate de prelucrare și transmitere a informației;
  - compromiterea cheilor și mijloacelor de protecție criptografică a informației;
  - sustragerea informației prin canale tehnice;
  - montarea ilegală a dispozitivelor electronice în mijloace tehnice de prelucrare, păstrare și transmitere a informației prin canalele de comunicații, precum și în încăperile de serviciu ale organelor puterii de stat pentru interceptarea informației;
  - nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau electronice;
  - interceptarea informației în rețelele de transmitere a datelor și pe liniile de comunicații, decodificarea acestei informații și impunerea informației false;
  - utilizarea tehnologiilor informaționale, a mijloacelor de protecție a informației, a mijloacelor de informatizare, de telecomunicații și comunicații necertificate, la crearea și dezvoltarea infrastructurii informaționale;
  - accesul neautorizat la resursele informaționale din băncile și bazele de date;
  - încălcarea restricțiilor legale privind răspîndirea informației.
  - atac asupra cheii / algoritm insuficient de puternic
  - analiza traficului
  - acces neautorizat la postul de muncă
  - acces neautorizat la rețea / resursele rețelei
  - canale ascunse (covert channels)
  - spoofing de rețea
  - viruși
  - spam
  - tunneling
  - atacuri de tip DoS (denial of service) - întreruperea serviciilor
  - repudiere.
- d) pericolele pentru securitatea informațională afectează:

- confidențialitatea informației;
  - integritatea logică și integritatea fizică a informației;
  - funcționarea normală a infrastructurii informaționale.
- e) pericolele pentru securitatea informațională pot fi realizate prin următoarele moduri:
- accesul neautorizat, ilegal sau nesancționat la resursele și infrastructura informațională;
  - influențarea fizică asupra componentelor infrastructurii informaționale;
  - organizarea ilegală a scurgerii informației prin diferite canale;
  - mituirea și/sau amenințarea personalului IFpS

**Standardele de referință pentru Sisteme informatice și e-Guvernare.**

***National Institute of Standards and Technology***

FIPS 140-2

Security Requirements for Cryptographic Modules

FIPS 180-2

Secure Hash Standard, August 2002

FIPS 186-2

Digital Signature Standard, February 2000

FIPS 188

Standard Security Label for Information Transfer

FIPS 196

Entity Authentication Using Public Key Cryptography

FIPS 197

Advanced Encryption Standard (AES)

SP 800-63

Electronic Authentication Guideline, Version 1.0.1

***Military Standards***

MIL-STD-498

Software Development and Documentation Standard, 1989

MIL-STD-810D (2)

Environmental Test Methods and Engineering Guidelines, 19 July 1983

***American National Standards Institute (ANSI)***

***International Organization for Standardization (ISO)***

***International Electro-technical Commission (IEC)***

ANSI/ISO/IEC TR 9294.1990

Information Technology Guidelines for the Management of Software Documentation

ISO/IEC TR 13335-4:2000

Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards

ISO/IEC TR 13335-3:1998

Information technology—Guidelines for the management of IT Security—Part 3 Techniques for the management of IT security

ISO/IEC TR 13335-2:1997

Information technology—Guidelines for the management of IT Security—Part 2: Managing and planning IT security

ISO/IEC TR 13335-1:1996

Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security

ISO 10007:1995

Quality Mgmt. Guidelines for Configuration Management

ISO 10005-1995

Quality Mgmt. Guidelines for Quality Plans

ANSI/ISO/ASQC QS9000-3-1997

QM and QA standards Part 3: Guidelines for the application of ANSI/ISO/ASQC Q9000-1994 to the Development, Supply, Installation, and Maintenance of Computer Software

***Electronic Industries Alliance Standards***

MB2, MB5, MB9

Maintainability Bulletins

EIA 157

Quality Bulletin

EIA QB2-QB5

Quality Bulletins

EIA RB9

Failure Mode and Effect Analysis, Revision 71

EIA SEB1—SEB4

Safety Engineering Bulletins

RS-232-C

Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange

RS-366-A

Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication

RS-404

Standard for Start-Stop Signal Quality Between Data Terminal Equipment and Non-synchronous Data Communication Equipment

NISTIR 4909

Software Quality Assurance: Documentation and Reviews

***National Institute of Standards and Technology***

***Institute of Electrical and Electronics Engineers***

610.12-1990

IEEE Standard Glossary of Software Engineering Terminology

730-1998

IEEE Standard for Software Quality Assurance Plans

828-1998

IEEE Standard for Software Configuration Management Plans

829-1998

IEEE Standard for Software Test Documentation

830-1998

IEEE Recommended Practice for Software Requirements Specifications

***Military Standards***

MIL-STD-498

Software Development and Documentation, 27 May 1998

***American National Standards Institute (ANSI)***

***International Organization for Standardization (ISO)***

***International Electro-technical Commission (IEC)***

ANSI/ISO/IEC TR 10176.1998

Information Technology Guidelines for the Preparation of Programming Language Standards

ANSI/ISO/IEC 6592.2000

Information Technology Guidelines for the Documentation of Computer Based Application Systems

ANSI/ISO/ASQC Q9000-3-1997

Quality management and quality assurance standards Part 3: Guidelines for the application of ANSI/IAO/ASQC Q9001-1994 to the Development, supply, installation and maintenance of computer software

ANSI/ISO/ASQC Q9000-1-1994

Quality Management and Quality Assurance Standards—Guidelines for Selection and Use

ANSI/ISO/ASQC Q10007-1995

Quality Management Guidelines for Configuration Management

ANSI X9.31-1998

Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998

ANSI X9.62-1998

Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, 1998

ISO/IEC 9594-8:2001

ITU-T Recommendation X.509 (2000), Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

***National Institute of Standards and Technology***

FIPS 102

Guideline for Computer Security Certification and Accreditation

FIPS 112

Password Usage (3)

FIPS 113

Computer Data Authentication

***Institute of Electrical and Electronics Engineers***

488-1987

IEEE Standard Digital Interface for Programmable Instrumentation

796-1983

IEEE Standard Microcomputer System Bus IEEE/ANSI Software Engineering Standards

750.1-1995

IEEE Guide for Software Quality Assurance Planning

1008-1987

IEEE Standard for Software Unit Testing

1016-1998

IEEE Recommended Practice for Software Design Descriptions

1012-1998

IEEE Guide for Software Verification and Validation Plans

***Other References***

Designing for the Color-Challenged: A Challenge, by Thomas G. Wolfmaier (March 1999);

[http://www.sandia.gov/itg/newsletter/mar99/accessibility\\_color\\_challenged.html](http://www.sandia.gov/itg/newsletter/mar99/accessibility_color_challenged.html);

Effective Color Contrast: Designing for People with Partial Sight and Color Deficiencies, by Aries Ardit, Ph.D; [http://www.lighthouse.org/color\\_contrast.htm](http://www.lighthouse.org/color_contrast.htm)

Electronic Markup Language (EML), Version 4.0, (Committee Draft) Organization for the Advancement of Structured Information Standards (OASIS), January 24, 2005

RSA Laboratories Technical Note, Public Key Cryptographic Standard (PKCS) #7: Cryptographic Message Syntax Standard, November 1, 1993

RSA Laboratories Technical Note, Extensions and Revisions to PKCS #7, May 13, 1997

The Americans with Disabilities Act Accessibility Guidelines (ADAAG 2202), Access Board;

<http://www.access-board.gov/adaag/html/adaag.htm>

**Lista formelor de declarații fiscale**

Taxa pe valoare adăugată

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/taxa\\_val\\_adaugata.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxa_val_adaugata.ascx)

Impozit pe proprietate [http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/improp.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/improp.ascx)

Impozit pe venit

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/impozit\\_pe%20venit.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impozit_pe%20venit.ascx)

Impozit privat [http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/impozit\\_privat.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impozit_privat.ascx)

Impozit pe resurse naturale

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/impoz\\_res\\_nat.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impoz_res_nat.ascx)

Taxa în fondul rutier

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/taxa\\_fond\\_rutier.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxa_fond_rutier.ascx)

Taxe locale [http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/taxe\\_locale.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxe_locale.ascx)

Dividende

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/doc/dividende/dividende.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/doc/dividende/dividende.ascx)

Accize [http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/accize.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/accize.ascx)

Taxe pe asistenta medicala

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/CNAM.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/CNAM.ascx)

Prime pe asistenta sociala

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/CNAM.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/CNAM.ascx)

Mărci de stat la producție alcoolică

[http://www.fisc.md/INDEX\\_main.aspx?source=doc/ro/declaratii/msta.ascx](http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/msta.ascx)